

**VŠB -Technická univerzita Ostrava**  
**Fakulta elektrotechniky a informatiky**  
**Katedra elektroniky**

**Elektronické zabezpečovací systémy**  
**Electronics Security systems**

**2009/2010**

**Dan Raszka**

## **Prohlášení studenta**

„Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně.

Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.“

V Ostravě dne .....

.....

podpis

## **Poděkování**

Děkuji vedoucímu bakalářské práce Ing. Petru Šimoníkovi, Ph.D. za jeho čas a ochotu poskytnout mi rady a připomínky v průběhu vypracování mé bakalářské práce.

## **Abstrakt**

Tato bakalářská práce se zabývá teoretickým rozбором koncepčních řešení elektrických zabezpečovacích systémů a vlastností dílčích komponentů a dále praktickou realizací vybrané koncepce zabezpečení. Ukazuje jakými způsoby lze zabezpečit objekty proti vniknutí nepovolených osob. Podává komplexní soubor informací o jednotlivých druzích ochrany objektů a prvcích elektrických zabezpečovacích systémů používaných k této ochraně.

Přehledným způsobem jsou v ní uvedeny teoretické i praktické poznatky z oboru elektrických zabezpečovacích systémů. Seznamuje s jejich doplňkovými zařízeními a s tím spojenými činnostmi a službami pro ochranu objektů a majetku.

## **Klíčová slova**

Elektrický zabezpečovací systém, čidlo, ústředna

## **Abstract**

The Bachelor's Thesis inquires into the solution of electric security systems and electrical properties of individual components and the practical implementation of selected concepts of security. It displays the methods of securing properties from trespassers' entry. It gives complex information on single types of property protection and electric security systems components used to the protection. Both the theoretical and practical findings from the area of the electric security systems are listed in a well-arranged way. The Thesis also acquaint with their complementary appliances and related activities and services for property and asset protection.

## **Keywords**

Electric Security System, Detector, Control panel

# OBSAH

<b>1 Úvod</b>	<b>8</b>
<b>2 Teoretická část</b>	<b>9</b>
2.1 Prvky prostorové ochrany (čidla prostorová)	9
2.1.1 Pasivní infračervená čidla	10
2.1.2 Ultrazvuková čidla	13
2.1.3 Mikrovlnná čidla	14
2.1.4 Kombinovaná (duální) čidla	15
2.2 Prvky plášťové ochrany	16
2.2.1 Magnetické kontakty	16
2.2.2 Čidla na ochranu skleněných ploch	17
2.2.3 Mechanické kontakty	17
2.2.4 Vibrační čidla	18
2.2.5 Poplachové fólie, tapety, polepy a poplachová skla	18
2.2.6 Drátová čidla	18
2.3 Prvky předmětové ochrany	18
2.3.1 Seismická (otřesová) čidla	19
2.3.2 Čidla na ochranu uměleckých předmětů	20
2.3.3 Kapacitní čidla	21
2.4 Prvky venkovní obvodové (perimetrické) ochrany	21
2.5 Ústředny EZS	23
2.5.1 Smyčková ústředna	23
2.5.2 Ústředna s přímou adresací čidel	24
2.5.3 Ústředny smíšeného typu (koncentrátorová)	25
2.5.4 Ústředny s bezdrátovým přenosem od čidel	25
2.5.5 Ústředny hybridní	28
2.5.6 Akustická signalizace	28
2.5.7 Optická signalizace	29
2.6 Napájecí zdroje ústředen	29
2.6.1 Základní síťový napájecí zdroj	29
2.6.2 Přídavný síťový napájecí zdroj	30
2.6.3 Náhradní (záložní) napájecí zdroj	30
2.7 Ovládací zařízení, propouštěcí zámky, indikační díly a systémy vstupu	31
2.7.1 Blokovací zámky	32
2.7.2 Spínací (propouštěcí) zámky	32
2.7.3 Kódové klávesnice	33
2.7.4 Kombinované indikační a ovládací díly	33
2.7.5 Ovládací prvky na bázi vstupních (propouštěcích) systémů	34
2.8 Prvky tísňového hlášení	34

2.8.1 Veřejné tísňové hlásiče .....	34
2.8.2 Speciální tísňové hlásiče .....	34
2.8.3 Automatické tísňové hlásiče .....	34
2.8.4 Osobní tísňové hlásiče .....	35
2.9 Přenos po síti GSM .....	35
2.10 Přenos bezdrátový .....	36
2.10.1 Přenos rádiový .....	37
2.10.2 Přenos optický .....	37
<b>3 Praktická část .....</b>	<b>38</b>
3.1.1 Technická dokumentace EZS .....	38
3.1.2 Schématické značky .....	39
3.1.3 Kalkulace nákladů na EZS .....	39
<b>4 Závěr .....</b>	<b>40</b>
<b>5 Literatura .....</b>	<b>41</b>
<b>6 Přílohy .....</b>	<b>42</b>
6.1 Uživatelský manuál .....	42

# 1 Úvod

Spolehlivost a význam elektrických zabezpečovacích systémů (EVS) v objektech se stále zdokonaluje. Z historického hlediska byly EVS druhou praktickou aplikací elektřiny vůbec.

V současné době tyto systémy expandují na trzích s elektrickými zařízeními a stále více se objevují nejen ve velkých firmách k ochraně jakýchkoli objektů, ale svou popularitu nacházejí i v soukromém sektoru. Elektrické zabezpečovací systémy jsou finančně dostupnější než by si leckdo myslel. Cenově jsou totiž srovnatelné s běžnými elektrickými spotřebiči. Jiná je ovšem hodnota systému, který je určen pro zabezpečení majetku, objektů a osob.

Cílem mé práce bylo detailně popsat veškeré dostupné kategorie EVS, význam a možnosti jejich komponentů a získat přehled o jednotlivých druzích EVS, jejich vlastnostech a praktickém využití při zabezpečení různých typů objektů.

Ve své práci jsem se věnoval elektronickému zabezpečení laboratoře automobilové techniky E118 na VŠB-TU v Ostravě. Prostudoval jsem různé typy a modifikace EVS, jejich klady i zápory. Z velké nabídky různých elektronických systémů jsem pro praktickou část vybral od firmy JABLOTRON elektronický zabezpečovací systém OASIS 868 MHz. Tento moderní bezdrátový systém je určen nejen k ochraně obytných prostor, obchodů nebo kanceláří, ale i skladů a dílen. Dokáže nejen hlásit vloupání, požár a zatopení vodou, ale i nebezpečí přehřátí, přepadení a další vzniklá rizika. Předností tohoto systému je ovládání až padesáti číselnými kódy nebo mobilním telefonem, popř. internetem, má unikátní bezdrátové detektory pohybu se zabudovanou kamerou.

## 2 Teoretická část

### 2.1 Prvky prostorové ochrany (čidla prostorová)

Prostorová ochrana tvoří velice dobrou alternativu, popř. doplnění k současně nejlepší formě střežení – plášťové ochraně. [1]

#### **Základní dělení:**

- Čidla pasivní – při zjišťování charakteristických rysů napadení registrují pouze fyzikální změny ve svém okolí.
- Čidla aktivní - vytvářejí své pracovní prostředí aktivním působením na své okolí a detekují změnu takto vytvořeného fyzikálního prostředí. [1]

#### **V praxi se setkáváme s několika druhy čidel pohybu:**

- Pasivní infračervená čidla (Passive Infra Red – PIR)
- Aktivní ultrazvuková čidla (Ultrasonic –US)
- Aktivní mikrovlnná čidla (Microwave – MW)
- Duální (Kombinovaná) čidla (PIR – US, PIR – MW) [1]

Každý z těchto čidel využívá ke své funkci odlišnou část kmitočtového spektra elektromagnetického vlnění. Ultrazvuková čidla využívají vlnění mechanické.

Každý druh čidla má určité vlastnosti, které jsou výsledkem úrovně vývoje zpracování signálu a výsledkem úrovně technologie daného výrobce. Vedle základních typů se na trhu objevují i různé modifikace využívající stejné fyzikální principy, ale doplněné speciálními funkcemi pro zpracování signálu. Velice často se zde objevují v sortimentu PIR čidel funkce počítání impulzů nutných k vyhlášení poplachů. Často jsou aplikovány pyrosenzory v dvojitém či čtyřnásobném provedení s paralelním vyhodnocením. Tyto funkce při vlastní aplikaci přinášejí vyšší odolnost proti falešným poplachům způsobeným vlivem okolí (proudění vzduchu, osvětlení, atd.). Tyto čidla však nepřinášejí vyšší úroveň bezpečnosti z hlediska napadení. Správně aplikované čidlo jednoduššího technologického provedení může uživateli sloužit stejně spolehlivě při nižších nákladech při pořízení. Jsou však objekty kde se bez čidel spolehlivějších a odolnějších proti vlivu okolí neobejdeme. Tyto čidla jsou ovšem dražší. [1]

#### **Některé typy čidel nabízejí další luxusní funkce:**

- Dálkové odpínání indikační LED – usnadní montážní organizaci uživateli testování funkce a dosahu čidel v provozu, při servisních zásazích a při pravidelných revizích a kontrolách.



- Odpínání mikrovlnné či ultrazvukové vysílací části čidel – u citlivějších osob může dojít ke zdravotním potížím při dlouhodobém pobytu v prostorech s ultrazvukovým nebo mikrovlnným polem.
- Paměť poplachu a dálkový reset této paměti – umožní identifikaci narušení prostoru nebo poruchu čidla v případech, je-li na jedinou smyčku připojeno více těchto čidel.[1]

Další doplňkovou funkci přinášející vyšší úroveň bezpečnosti, je funkce ochrany proti zastínění (antimasking). Funkce je aktivní i v době klidu objektu, slouží k indikaci zastínění čidla. Čidla s takovou funkcí jsou nasazeny v prostorech veřejně přístupných, kde je riziko sabotáže systému s cílem připravit si objekt na vloupání ve stavu střežení. Výstup této indikace bývá projektován dle použitého typu ústředny a režimu objektu na samostatnou smyčku nebo bývá funkčně spojen s příslušnou poplachovou smyčkou do které je dané čidlo připojeno. Důvody pro nasazení čidel s funkcí antimasking mohou být dva:

- Objektu se strážní službou (stálou nebo denní) - požadavek okamžité indikace zastínění čidla nebo jeho přestříkání barvou.
- V objektu bez strážní služby – požadavek zabránění uvedení do stavu střežení, pokud je některé z čidel s funkcí antimasking zastíněno.[1]

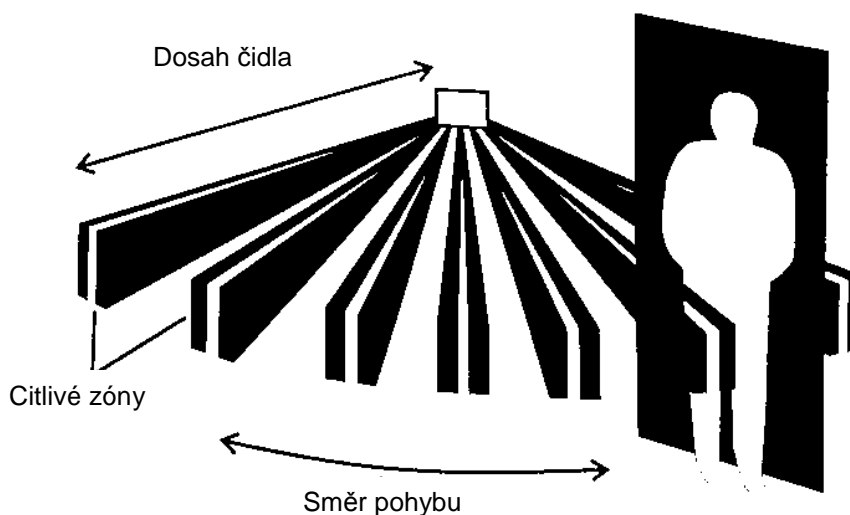
### 2.1.1 Pasivní infračervená čidla

#### Princip funkce a praktické provedení

Tato čidla jsou označována jako PIR čidla. Založená jsou na principu zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Pracují na základě skutečnosti, že každé těleso, mající teplotu vyšší než  $-273^{\circ}\text{C}$  (absolutní nula) a nižší než  $560^{\circ}\text{C}$ , je zdrojem vyzařování vlnění v infrapásmu odpovídajícím teplotě tělesa.

Směrem k vyšším teplotám se posouvá spektrum ke kratším vlnovým délkám, tedy k oblasti viditelného spektra. Takové vlnění přestáváme vnímat jako teplo a začínáme je vnímat jako světlo. Vlnová délka 9,4 mm je charakteristická pro teplotu lidského těla cca  $35^{\circ}\text{C}$ . Tento jev se využívá k zachycení pohybu těles, které mají odlišnou teplotu od teploty okolí. Jako detektor se používá materiál vykazující pyroelektrický jev. Detekční prvek je měnič gradientní povahy, tzn. že není schopen detekovat stálou úroveň záření, ale jen změny záření na detektor dopadajícího. Na plochu senzoru prostřednictvím optiky je transformován obraz střeženého prostoru v infračerveném pásmu. Na aktivní a neaktivní zóny je rozděleno zorné pole, které si můžeme představit jako viditelné a zakryté části obrazu střeženého prostoru. Pokud se pohybuje v zorném poli čidla PIR pohybuje těleso, jehož teplota je odlišná od teploty okolí (pozadí), zachycuje čidlo změny při přechodu cíle z aktivní do neaktivní zóny a naopak. Elektronika vyhodnotí signál vyvolaný těmito změnami a způsobí vyhlášení poplachu. Na provedení optiky je závislý tvar zorného pole. Dosah je závislý na kvalitě

optiky čidla, citlivosti použitého senzoru a způsobu vyhodnocení. Správnou volbou optiky je možné střežit prostor do vzdálenosti cca 15 m od čidla nebo též dlouhé prostory do cca 60 m. U čidel pro stropní montáž lze kruhovým uspořádáním optiky obsáhnout plochu v rozsahu 360°. [1]



Obr.1 Princip zachycení pohybu PIR čidlem [1]

V praxi se setkáváme s optikou dvojího druhu:

- soustava Fresnelových čoček
- soustava křivých zrcadel [1]

Optika vždy transformuje obraz zorného pole do podoby, který dalšímu elektrickému zpracování výstupního signálu pyrosenzoru vyhovuje nejlépe. [1]

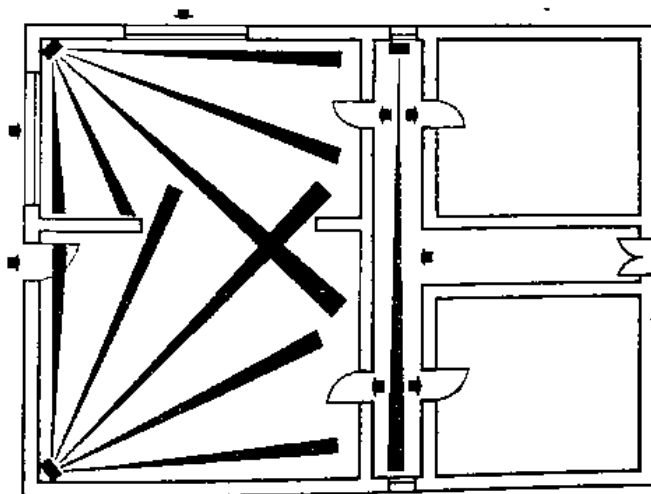
#### Porovnání obou druhů optiky:

- I přes určité nedostatky způsobené tím, že zobrazení pomocí Fresnelových čoček nedává ideální optický obraz, je toto řešení velice ekonomické.
- I přes náročnější návrh a technologii výroby je optický obraz vytvořený pomocí křivých zrcadel zobrazením bez kompromisu.[1]

Se zrcadlovou optikou se setkáváme především u čidel tradičních značkových výrobců. Na trhu se můžeme setkat i s alternativou tzv. černých zrcadel, která omezují odrazivost v oblastech mimo požadované infračervené spektrum. Tímto řešením je podstatně snížena náchylnost čidel k planým poplachům, jenž jsou způsobeny zářením o vysoké energii ve viditelném spektru, jako jsou odlesky slunce, reflektory automobilů apod. [1]

## Použití a montáž

Těžištěm prostorové ochrany jsou centrální body budovy – spojovací chodby, haly, schodišťové přístupy a výstupy a vnitřní komunikační uzly. Díky menší náročnosti na montáž je nahrazena plášťová ochrana ochranou prostorovou. V objektech s nízkými riziky napadení a při umístění čidel v místech kde skutečně pokrývají nejpravděpodobnější místa vniku z vnitřní strany pláště objektu, je možno tento ekonomický argument připustit. Plně nahradit plášťovou ochranu však nikdy nemůže. [1]



Obr.2 Příklad správného umístění PIR čidel [1]

### Zásady instalace PIR čidel:

- PIR čidla se instalují tak, aby pravděpodobný směr pohybu pachatele byl kolmý na myšlený průmět aktivní či neaktivní zóny střeženého prostoru.
- Předpokladem spolehlivé funkce veškerých prostorových čidel je jejich umístění na stavebně pevném podkladu bez vibrací.
- Více PIR čidel lze instalovat bez nebezpečí vzájemného ovlivňování do jednoho prostoru, protože nevyzařují žádnou energii.
- PIR čidlo je aktivováno pouze tangenciální složkou pohybu pachatele ve vztahu k rozložení aktivních a neaktivních zón. Doporučuje se proto v případě nutnosti úplného pokrytí prostoru instalace více čidel pro vzájemné překrytí zón.
- PIR čidla neinstalujeme v prostorách s podlahovým vytápěním.
- PIR čidla nesmějí být nasměrována na okna, vnější dveře a vrata.[1]

### Kritéria falešných poplachů

PIR čidla nesmějí být vystavena těmto vlivům:

- Přímé nebo nepřímé vyzařování světla (slunce, reflektory apod.)
- Proměnné zdroje tepla (topení, komíny)

- Ventilace (vstupy, výstupy, průvan)
- Spínané rušivé IR zdroje (žárovky)[1]

### **Nastavení, údržba**

K nastavení jednotlivých typů PIR čidel používáme instalační manuál výrobců. Většina PIR čidel nemá funkce pro jemné nastavení dosahu čidla. Je možné však přizpůsobit snímací charakteristiku výšce montáže čidla. Technicky je pak snímací charakteristika naklápěná v rozmezí jednotek stupňů vertikálním posunem celé desky elektroniky v krytu čidla nebo naklápěním soustavy křivých zrcadel.

Při pravidelné údržbě kontrolujeme, zda čidlo není zastíněno změnami v interiéru (závěsy, záclony, žaluzie, skříně apod.). Je nutno pravidelně ověřovat dosah čidla z důvodu jeho zašpinění či zaprášení Fresnelovy čočky nebo zrcadlové optiky. V neposlední řadě patří k pravidelné kontrole i funkce zajišťovacího kontaktu krytu čidla. [1]

## **2.1.2 Ultrazvuková čidla**

### **Princip, funkce a praktické provedení**

Ultrazvuková čidla (Ultrasonic sensor – US) využívají část spektra mechanického vlnění nad pásmem kmitočtu slyšitelných lidským uchem. Jsou aktivní – do prostoru vysílají energii. Vysílač vlnění vysílá vlnění o stálém kmitočtu. Přijímač toto vlnění odrážené od překážek v uzavřeném prostoru přijímá. V klidovém stavu je přijatá vlna vyhodnocena elektronikou pohybuje-li se v prostoru libovolné těleso, mění se fáze přijatého vlnění. Tuto změnu fáze vyhodnocuje elektronika a vyhlašuje poplach. [1]

### **Použití a montáž**

- US čidla pohybu instalujeme tak, že pravděpodobný pohyb pachatele směřuje k čidlu nebo od něj. Typický dosah je do 10 m.
- Prostor musí být uzavřený, dosah čidla nemůže přesahovat mimo prostor určený ke střežení.
- V prostorách s často se měnícím stavem interiéru upouštíme od montáží US čidel.
- Předměty umístěné do blízkosti čidel až po jejich instalaci a nastavení mohou způsobovat falešné poplachy ovlivněním citlivosti čidel.
- V prostorách, kde jsou uloženy koberce nebo pěnové materiály absorbující ultrazvuk, musíme počítat s tím, že se citlivost US čidel může značně změnit oddálením nebo přiblížením těchto předmětů. Vzniká nebezpečí, že čidlo bude po změně příliš citlivé nebo málo citlivé. [1]

## **Kritéria falešných poplachů**

Více US čidel pohybu v jednom prostoru můžeme instalovat jen tehdy, jsou-li vysílače synchronizovány nebo kmitočtově stále, bez vzájemného negativního ovlivňování. US čidla pohybu nesmíme instalovat:

- Na zavěšené montážní konstrukce.
- V prostorách s teplovzdušným topením
- Nad topná tělesa
- V blízkosti zdrojů zvuků se širokým kmitočtovým spektrem, např. telefon.
- V prostorách, kde se pohybují v době střežení zvířata.
- V prostorách s volně zavěšenými předměty, např. lampy, reklamní štíty.[1]

## **Nastavení a údržba**

Při nastavování postupujeme od nejmenšího dosahu. V momentě, kdy dosáhneme požadovaného pokrytí, výkon ultrazvukového měniče již nezvyšujeme. Čidlo má tak optimální dosah při minimální náchylnosti k falešným poplachům. [1]

Při pravidelné údržbě kontrolujeme, zda se nezměnily akustické vlastnosti prostoru, v němž je čidlo nasazeno. Při jakékoli změně v interiéru je pak třeba dosah čidel znovu nastavit. K pravidelné kontrole patří samozřejmě i kontrola funkce zajišťovacího kontaktu krytu čidla.[1]

## **2.1.3 Mikrovlnná čidla**

### **Princip funkce a praktické provedení**

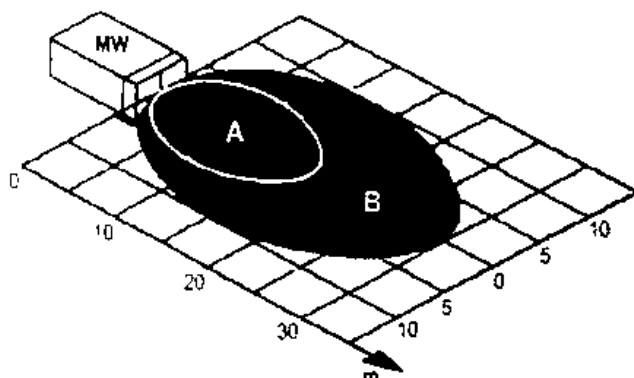
Mikrovlnná čidla (microwave senzore-MW) vycházejí ze stejného fyzikálního principu jako ultrazvuková čidla, ale v kmitočtovém pásmu elektromagnetického vlnění. Jedná se většinou o pásma 2,5 GHz, 10 GHz nebo 24 GHz. Je to aktivní systém zachycení pohybu, principiálně shodný s ultrazvukovými čidly. Je však technologicky uzpůsoben danému kmitočtovému pásmu. Nejčastěji užívané pásmo X je shodné např. s pásmem družicové televize. [1]

### **Použití a montáž**

MW čidla pohybu instalujeme tak, aby pravděpodobné směry pohybu pachatele vedly k čidlu nebo od něho radiálně.

Čidla se musí instalovat tak, aby podněty mimo střežený prostor neovlivňovaly činnost čidla. Protože mikrovlny pronikají skleněnými plochami, tenkými stěnami ze dřeva, tvrzeného

papíru nebo plastické hmoty. Pohyby mimo střežený prostor mohou vést k aktivaci mikrovlnného čidla. [1]



Obr.3 Charakteristika mikrovlnného čidla ve volném prostředí (A varianta s nižším dosahem, B varianta s vyšším dosahem) [2]

### Kritéria falešných poplachů

- V blízkosti MW čidel se nesmí nacházet žádné velké objekty z kovu. Zvlášť kritické jsou objekty s rovinným povrchem, od kterého se mikrovlny odrážejí a mění tím výrazně detekční charakteristiku.
- MW čidla nemůžeme instalovat v prostorách, kde může ve stavu střežení objektu docházet ke spínání zářivkového osvětlení. V jednom prostoru můžeme použít více MW čidel jen tehdy, pracují-li na jiné vysílací frekvenci nebo jsou aplikovány tak, že je vyloučeno jejich vzájemné negativní ovlivňování.[1]

### Nastavení, údržba

Nastavení vychází z instalačních manuálů výrobců jednotlivých typů MW čidel. Můžeme říct, že všechna MW čidla mají možnost jemného nastavování dosahu čidla. Při nastavování postupujeme od nejmenšího dosahu. V okamžiku, kdy dosáhneme požadovaného pokrytí, výkon mikrovlnného měniče již nezvyšujeme. V tomto stavu má čidlo optimální dosah. Při minimální náchylnosti k falešným poplachům. V rámci pravidelné údržby musíme kontrolovat, zda nedošlo ke změně elektromagnetických vlastností prostoru, kde je čidlo osazeno. Ty mohou být ovlivněny změnami v interiéru, jako jsou velké kovové předměty (sítě, mříže, oplechované dveře). Při takovýchto změnách interiéru musíme vždy dosah čidel znovu nastavit. [1]

### 2.1.4 Kombinovaná (duální) čidla

V prostorách s výrazným negativním vlivem okolního prostředí, lze využít kombinovaných čidel PIR-US nebo PIR-MW. Vlastní myšlenka pro vývoj kombinovaných čidel vychází ze zásady, že je zanedbatelná pravděpodobnost současného vzniku jevů, které by mohly vyvolat planý poplach u více čidel pracujících na různých fyzikálních principech. Tato aplikace

snižuje rizika falešných poplachů vlivem prostředí známá u jednosystémových čidel, protože rizikové faktory falešných poplachů se pro jednotlivé systémy liší. [1]

### **Použití a montáž**

Při instalaci kombinovaných čidel musíme vycházet z pravidel, která jsou platná pro jednotlivé systémy v užitých čidlech. Jejich nasazení použijeme jen při nepříznivých podmínkách s ohledem na vyhlásování planých poplachů. Musíme si uvědomit, že práh detekce je u těchto čidel posunut poněkud výše oproti jednosystémovým čidlům. [1]

## **2.2 Prvky plášťové ochrany**

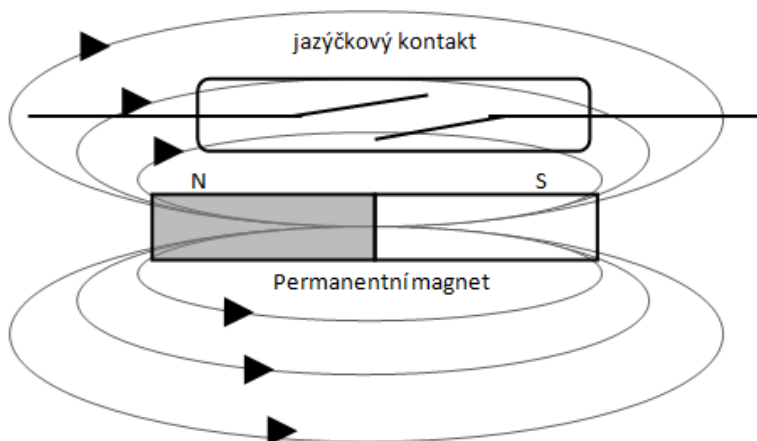
Úkolem prvků EZS v plášťové ochraně je včasná signalizace snahy pachatele o překonání klasické ochrany chráněného objektu. Jedná se především o vnější odporové výplně (dveře, okna) a o stavební prvky budov (obvodové zdivo, stropy, střechy, podlahy).[1]

### **2.2.1 Magnetické kontakty**

Magnetické kontakty tvoří vždy dvojice dílů – jazýčkový kontakt a permanentní magnet.

-jazýčkový kontakt: zatavená skleněná trubička naplněna ochrannou atmosférou, kde jsou umístěny dva feromagnetické kontakty.

- permanentní magnet: zmagetizovaný váleček z feritu (ALNICO) . [1]



Obr.4 Princip funkce magnetického kontaktu [1]

Klidový stav – kontakt jazýčkového relé je sepnut magnetickým polem permanentního magnetu.

Aktivace – oddálením magnetů se kontakt rozeptne, tím způsobí poplachové hlášení. Permanentní magnet i jazýčkový kontakt jsou samostatně zapouzdřeny do krytů z nemagnetického materiálu (plast, hliníkové slitiny). Skrytou montáž do tělesa dveří nebo

oken umožňují různá provedení magnetických kontaktů. Magnetický kontakt v těžkém klimaticky i mechanicky odolném provedení je určen ke střežení prostupů jež jsou opatřena roletami. Magnetické kontakty odolné proti magnetickému poli jsou určeny pro speciální aplikace s velmi vysokými riziky (např. věznice). Jakýkoliv pokus o odstavení magnetického kontaktu přiložením cizího magnetu vyvolá automaticky poplachové hlášení. Tyto speciální magnetické kontakty obsahují polarizovaný jazýčkový kontakt, nebo kontakt, který je tvořen sérioparalelní kombinací více kontaktů ( 3-7 jazýčkových kontaktů). Některé z nich jsou spínací a jiné rozpínací. [1]

### **2.2.2 Čidla na ochranu skleněných ploch**

Aktivní čidla na ochranu skleněných ploch jsou určena pro nejvyšší úroveň rizik. Obsahují vysílací i přijímací část. Elektronika vyhodnocuje změny přenosů oproti normálnímu stavu, který je uložen v paměti čidla. Tato čidla se vyznačují velkým dosahem střežení (až 25 m plochy dle typu čidla a typu skla). [1]

#### **Akustická čidla rozbití skleněných ploch**

Nevyhodnocují vlnění v tělese skla, ale akustický efekt při tříštění skla, který je naprosto charakteristický. U těchto čidel elektronika vyhodnocuje akustické vlnění přijaté elektretovým mikrofonom. [1]

Nejnovější typy těchto akustických čidel vyhodnocují zvukové spektrum ve více bodech a hlášení vyvolají až poté, co jsou všechny tyto zvukové kmitočty v určitém časovém intervalu obsaženy. Jedná se o zvuk tříštivého skla o vysoké frekvenci a přítomnost rázové vlny vyvolané borcením skleněné plochy v oblasti nízkých kmitočtů. [1]

#### **Principy funkce a praktické provedení**

Tříštění skla vyvolává charakteristický zvuk. Ten se hmotou skla šíří jako vlnění v pevném tělese. Toto vlnění zachycuje čidlo, které je spojeno s plochou skla – tzv. kontaktní čidlo. Při narušení skleněné plochy je elektronikou čidla vyhodnoceno vlnění – čidlo způsobí hlášení. Podle konstrukce čidla dojde k rozepnutí bezpotenciálového kontaktu relé, jenž je zapojen v poplachové smyčce, nebo o prudký nárůst odběru čidla, které je napájeno z poplachové smyčky. Dosah těchto čidel je 1,5 – 3 m. [1]

### **2.2.3 Mechanické kontakty**

Mechanické kontakty jsou mikropsínačem, které jsou konstrukčně uzpůsobené pro zabudování do rámu proti západce zámku. Jsou určeny ke střežení uzamčeného stavu prostupů. Při vhodném zapojení k ústředně EZS zabrání uvedení do stavu střežení v případě, že některý z prostupů není uzamčen. Tyto mechanické kontakty se užívají v případech, jestliže střežený prostor má více



vstupů. Mezi mechanické kontakty řadíme i nájezdy, které umožňují uzavřít elektrický obvod tam, kde je třeba přivést proud do čidla na otočný nebo posuvný díl osazení stavebního otvoru. Nájezd současně plní funkci střežení daného prostupu na jeho otevření. [1]

#### **2.2.4 Vibrační čidla**

K prvkům střežení pláště budov rovněž patří vibrační čidla. Jsou určena k hlídání průrazu stěn a stavebních konstrukcí. Základem těchto čidel je elektromechanický měnič, který je doplněn vyhodnocovací elektronikou. Čidla mají větší šířku pásma vyhodnocovaných kmitočtů. Dále mají optickou indikaci s pamětí a nastavitelnou citlivost. Čidla jsou osazována na riziková místa možného průchodu zdí (luxfery, rámy dveří a oken). Vzhledem ke své konstrukci nemohou být určena ke střežení komorových trezorů a trezorových skříní. [1]

#### **2.2.5 Poplachové fólie, tapety, polepy a poplachová skla**

Jsou to čidla pracující na principu přerušení vodivého média. Nejčastěji se používá jemného drátku uvnitř zmiňovaného nosiče (fólie, tapety, skla), nebo pásků vodivé fólie které jsou umístěny na povrch hlídané plochy (polepy). Při montáži je důležité orientovat připojené místo k horní hraně plochy tak, aby bylo chráněno před možnou kondenzací páry. Ta může snížit životnost nebo spolehlivost spojení. [1]

#### **2.2.6 Drátová čidla**

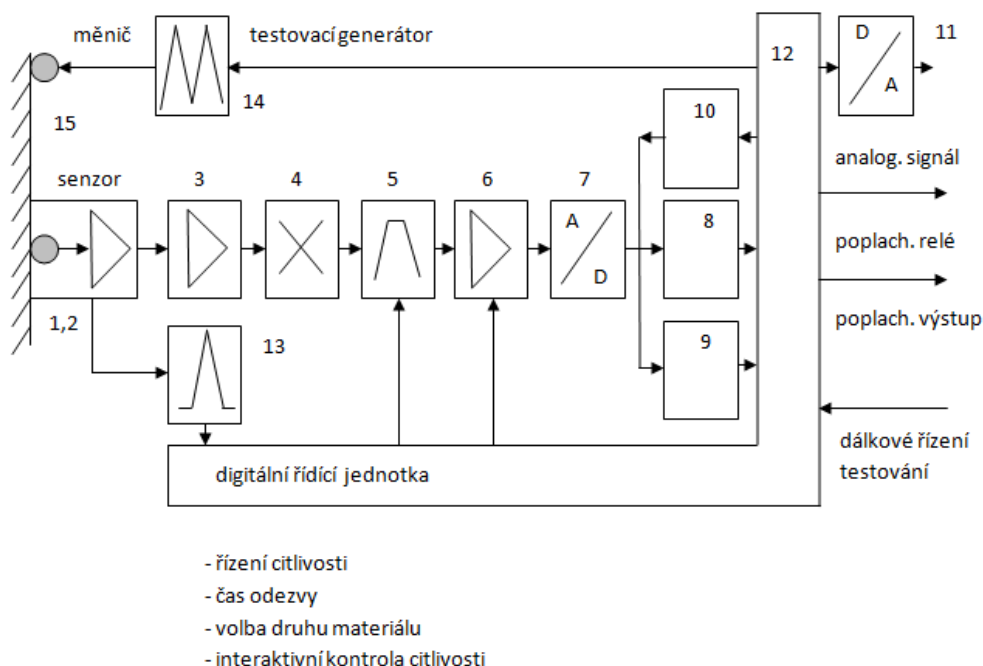
Drátová čidla jsou jemná ocelová lanka propojená s citlivým mikrosplínáčem. Používají se ke střežení velkých prostupů ventilace a prostupů inženýrských sítí do objektů. Pro usnadnění montáže jsou výrobci nabízena rozsáhlá příslušenství prostředků k jejich upevnění. Správně instalovaná drátová čidla reagují již na slabé zvýšení mechanického napětí. [1]

### **2.3 Prvky předmětové ochrany**

Pro předmětovou ochranu lze použít prvky, které byly původně určeny pro jiné účely (např. magnetické kontakty, PIR čidla s charakteristikou záclona, infračervené závory, reflexní optoelektronická čidla, mikrovlnná čidla aj.). Pro střežení komorových trezorů a trezorových skříní byla speciálně vyvinuta seismická čidla. Další skupinu předmětových čidel tvoří specifické závěsové a polohové čidla k ochraně uměleckých předmětů. [1]

### 2.3.1 Seismická (otřesová) čidla

Seismická (otřesová) čidla pracují na principu selektivního zpracování vlnění, které se šíří pevnými tělesy při jejich mechanickém nebo termickém opracovávání. Moderní typy těchto čidel využívají při své činnosti digitálního zpracování signálů. [1]



Obr.5 Blokové schéma otřesového čidla

#### Popis funkce otřesového čidla s digitálním zpracováním signálu:

Vlnění z tělesa snímá seismický detektor (1). Elektronika selektivně zpracovává a vyhodnocuje podněty z okolí. Po impedančním přizpůsobení mikrofonu (2) postupuje signál do předzesilovače (3), potom je ve směšovači (4) převeden na mezifrekvenční signál. Signál je dále vyfiltrován v pásmové propusti (5), zesílen v zesilovači (6) a převeden v převodníku (7) na digitální signál. Další zpracování je vedeno pouze v digitální podobě:

- digitální integrátor (8)
- digitální úrovňový analyzátor (9)
- digitální regulátor (10)

Mikroprocesorová jednotka (12) řídí všechny tyto operace. Do analogové podoby je převeden digitální výstup v převodníku (11) a je využitý k řízení standardních výstupů (poplachové relé, analogový výstup pro kontrolu snímání, výstup otevřeného kolektoru apod.)

Samostatný kanál slouží pro podněty velké amplitudy (13). Jeho výstup je přímo analyzován digitální řídicí jednotkou. Zabudovaný testovací generátor (14) a testovací elektroakustický měnič (15) slouží k testování funkce čidla. Velkou a podstatnou výhodou otřesových čidel je skutečnost, že k vyhlášení poplachu dojde dříve, než se pachatel zmocní cenných předmětů

umístěných v chráněném prostoru. Otřesová čidla reagují s maximální přesností na všechny známé druhy napadení skříňových trezorů, peněžních automatů, nočních trezorů a těžkých trezorových místností. Reagují na mechanické i termické napadení, jako je: [1]

- užití hrubého mechanického nářadí
- vrtání pomocí vrtáku s diamantovou korunkou
- užití hydraulického tlakového nářadí
- řezání kyslíko-vodíkovým plamenem
- použití plastických a jiných trhavin [1]

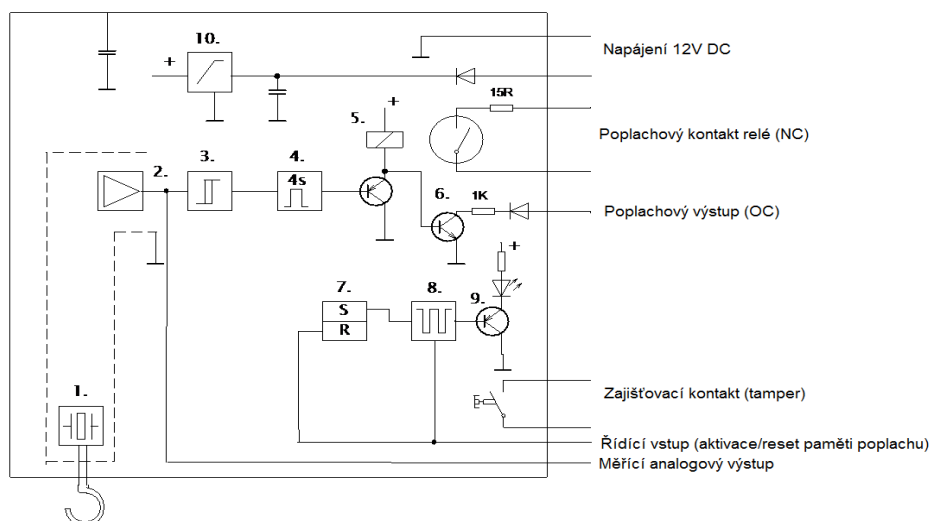
### 2.3.2 Čidla na ochranu uměleckých předmětů

Jsou určena pro střežení zavěšených uměleckých předmětů v galeriích, muzeích atd. Princip činnosti umožňuje trvalý provoz střežení. Tato čidla dělíme do dvou skupin:

- závěsová čidla
- polohová čidla [1]

#### Závěsová čidla:

na hák čidla je zavěšen pomocí závěsného lanka střežený předmět. Čidlo vyhodnocuje síly působící na hák a elektronika podle nastavení citlivosti vyhodnotí i velmi malé pohyby střeženého předmětu, pokus o jeho sejmutí nebo jen pouhý dotek. Jedná se o elektromechanický měnič doplněný vyhodnocovací elektronikou s nastavitelnou citlivostí. Háček je propojen s piezokeramickým měničem (1), signál narušení je zesílen v zesilovači (2), tvarován a filtrován (3), ovládá monostabilní klopný obvod (4) a výkonovou elektroniku relé (8). Další obvody slouží k filtraci napájení (10), řízení indikace a paměti poplach (6,7,8,9).[1]



Obr.6 Blokové schéma závěsového čidla

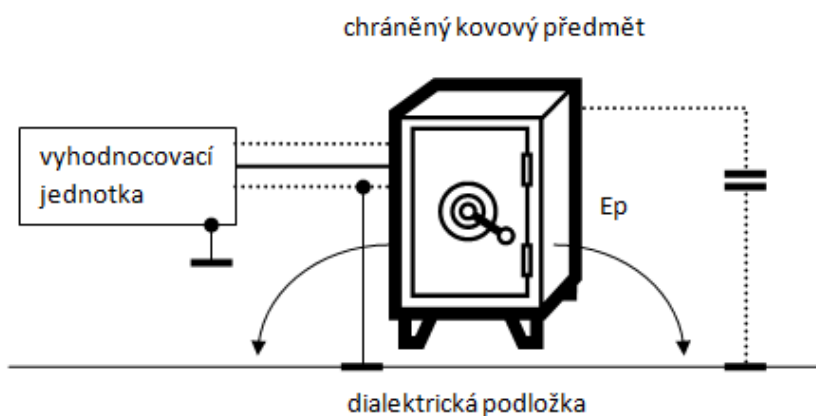
### Polohová čidla:

elektromagnetiká nebo kontaktní čidla reagující velmi citlivě na změnu polohy střeženého předmětu. Vychýlením „praporku“ čidla, které se přímo dotýká části střeženého předmětu (plátno, obraz, gobelín) mimo stanovený rozsah se aktivuje magnetický kontakt a elektronika čidla vyhlásí poplach. Tento typ čidla je využíván v případech, kde nelze použít čidla závěsová.[1]

### 2.3.3 Kapacitní čidla

Kapacitní čidla jsou určena k indikaci přiblížení nebo doteku chráněného předmětu. Používají se k ochraně obrazů, volně stojících předmětů a kovových i nekovových skříní.

V elektrickém poli čidla ( $E_p$ ) je umístěn střežený předmět. Osoba v elektrickém poli kondenzátoru tvořeného střeženým předmětem a polepy mění parametry dielektrika (okolní vzduch), a tím i kmitočet oscilátoru, jehož součástí je kondenzátor. Tyto změny vyhodnocuje fázový detektor a dává povel k vyhlášení poplachu.[1]



Obr.7 Princip funkce kapacitního čidla

## 2.4 Prvky venkovní obvodové (perimetrické) ochrany

Čidla, která chrání (signalizují) narušení vnějších částí rozlehlých objektů, komplexu budov nebo továren na samostatném pozemku. [1]

Je řada druhů čidel založených na různých fyzikálních principech, z nichž každé je určeno pro specifickou povahu chráněného pozemku. Liší se podle účelu nasazení a stupně důležitosti zabezpečení. [1]

Konstrukce vnějších čidel, zvláště mechanické a klimatické krytí, odpovídá vnějšímu prostředí. Tak se odlišuje od částí zabezpečovacího systému, které je umístěno uvnitř budov. [1]

Vzhledem k odlišným dimenzím venkovních ploch se liší od čidel pro vnitřní použití především v dosahu. Funkční dosahy vnitřních čidel se řádově pohybují kolem 10m.[1]

U venkovních čidel se však jedná o 100 m. Dalším rozdílem je tvar střeženého prostoru. Pokud je možnost přiblížení se k objektu z více stran, je vhodnější chránit celý plošný rozměr prostoru a zároveň mít možnost přímé adresace pro každý bod chráněné plochy. [1]

Jedna z hlavních podmínek při užití venkovní obvodové ochrany, aby bylo možno definovat narušení, je existence oplocení. Bez této mechanické zábrany by mohlo docházet k nechtěnému vstupu nepovolaných osob na zabezpečený pozemek. Při signalizaci poplachu by byl zákrok a postih z právního hlediska velmi problematický. [1]

K dalším problémům venkovního zabezpečení patří velké množství podnětů na které by neměla čidla reagovat. Mezi rušivé vlivy patří:

- Vlnění travního porostu
- Pohyb listí a větví stromů a keřů
- Vibrace oplocení ve větru
- Vítr, sníh a déšť
- Proudění vzduchu
- Pohyby různých druhů zvěře
- Dopravní ruch v blízkosti hranice pozemku[1]

Tyto vlivy mohou způsobovat falešné poplachu. Vhodný výběr varianty střežení venkovního perimetru musí vycházet z přesné a důkladné znalosti zabezpečovaného objektu. Podněty, které svým charakterem se přibližují k situaci narušení, nelze nikdy zcela eliminovat. Z těchto a jiných důvodů se proto kombinuje systém venkovní perimetrické ochrany se systémem průmyslové televize (CCTV). [1]

Hlavním požadavkem na prvky venkovní perimetrické ochrany je nezávislost funkce na klimatických podmínkách. Venkovní čidla proto bývají obvykle vybavena vnitřním vyhříváním. Kryty čidel a vyhodnocovací elektroniky musí být dokonale utěsněny. Jejich kontakty musí být zapojeny do zajišťovací smyčky. Taktéž přívodní kabely musí být kvalitně utěsněny v průchodkách do krytu čidel a vyhodnocovací elektronické jednotky. [1]

V současné době se nabízí rozsáhlý sortiment prvků venkovní perimetrické ochrany. Každý z těchto prvků má podle použitého fyzikálního principu své výhody i nevýhody. Volba vhodného typu pro konkrétní zabezpečení proto závisí na zkušenostech a odborných znalostech projektanta. [1]

## 2.5 Ústředny EZS

### Základní funkce a rozdělení ústředn EZS

Ústředna elektrické zabezpečovací signalizace je zařízení, které:

- Přijímá a vyhodnocuje výstupní elektrické signály od čidel EZS
- Napájí čidla a další prvky EZS elektrickou energií
- Ovládá signalizační, přenosová, zapisovací a jiná zařízení která indikují narušení
- Umožňuje uvedení celého systému EZS nebo jeho částí do stavu střežení nebo klidu pomocí elektromechanických nebo kódových zámků, popř. vlastních ovládacích klávesnic
- Umožňuje diagnostiku EZS[1]

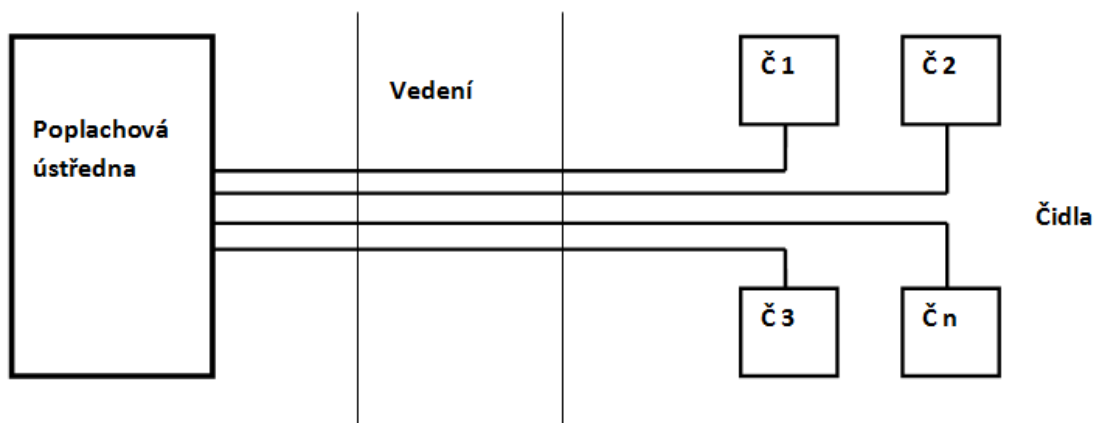
Ústředny EZS dělíme do čtyř hlavních skupin:

- ústředny smyčkové
- ústředny s přímou adresací čidel
- ústředny smíšeného typu
- ústředny s bezdrátovým přenosem poplachového signálu od čidel[1]

### 2.5.1 Smyčková ústředna

Má pro každou poplachovou smyčku vstupní vyhodnocovací obvod. Tento obvod je řešen pro připojení proudových smyček o definované hodnotě a toleranci. Smyčka je zakončena zakončovacím odporem tak, aby vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. K vyhlášení poplachového stavu systému EZS vede změna odporu smyčky, způsobena aktivací některého z čidel smyčky nebo sabotáží na smyčce. Poplachové smyčky systému EZS jsou tvořeny sériovým zapojením rozpínacích kontaktů čidel. [1]

Systém EZS se smyčkovou ústřednou má rozsáhlou kabelovou síť. To proto, že ke každému čidlu musí být přiveden kabel příslušné smyčky. Musí obsahovat dva vodiče pro napájení čidla, dva vodiče pro poplachový kontakt čidla, dva vodiče pro sabotážní kontakt čidla a vodiče dodatkových funkcí - paměť poplachu, test chůzí, odpojení vysílače ultrazvuku nebo mikrovlnného výkonu, indikace překrytí čidla apod. [1]

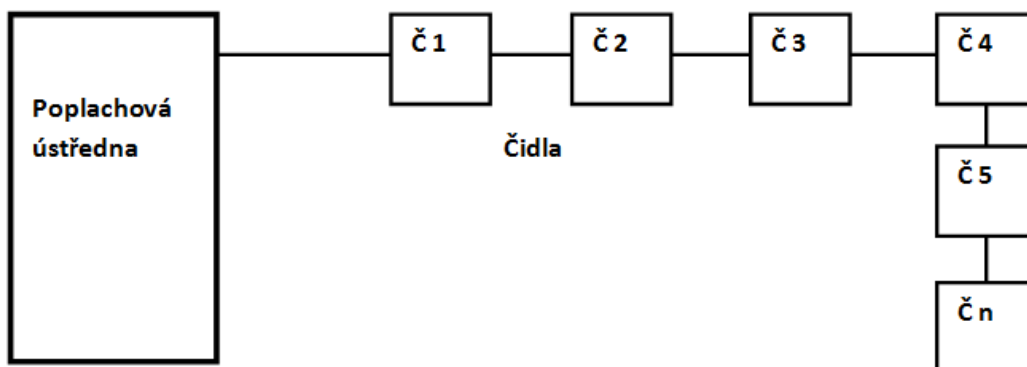


Obr.8 Příklad propojení zabezpečovacího systému se smyčkovou ústřednou

### 2.5.2 Ústředna s přímou adresací čidel

Ústředna pracuje na principu komunikace po datové sběrnici ústředna – čidla. Ústředna periodicky generuje adresy jednotlivých čidel a přijímá příslušné odezvy. Každé čidlo je vybaveno komunikačním modulem. Kabelová síť tohoto systému je minimální, protože je tvořena libovolnou konfigurací kabelové sítě. Jednotlivá čidla jsou připojena v libovolném pořadí na čtyřvodičové vedení. Dva vodiče slouží pro napájení čidla a dva jako datová sběrnice. Výhodou tohoto systému je, že při narušení objektu ústředna oznámí, které konkrétní čidlo bylo aktivované a jaký je druh narušení (zkrat na lince, sabotážní kontakt, poplachový kontakt apod.). [1]

Tento systém přináší výhody uživateli v případě, že je v objektu místo trvalé obsluhy nebo je-li přenos na PCO, popř. monitorovací pult hlídací služby realizován jako mnohokanálový. Jednoduchost kabelové sítě je však vykoupená nemožností realizovat po datové sběrnici dodatkové funkce čidel. Konfigurace kabelové sítě má rovněž své omezení. Jedním z nich je celková délka vedení, dále je nutné vyvarovat se uzavřených okruhů přes nezanedbatelnou plochu, do které by se mohlo indukovat elektromagnetické rušení. [1]

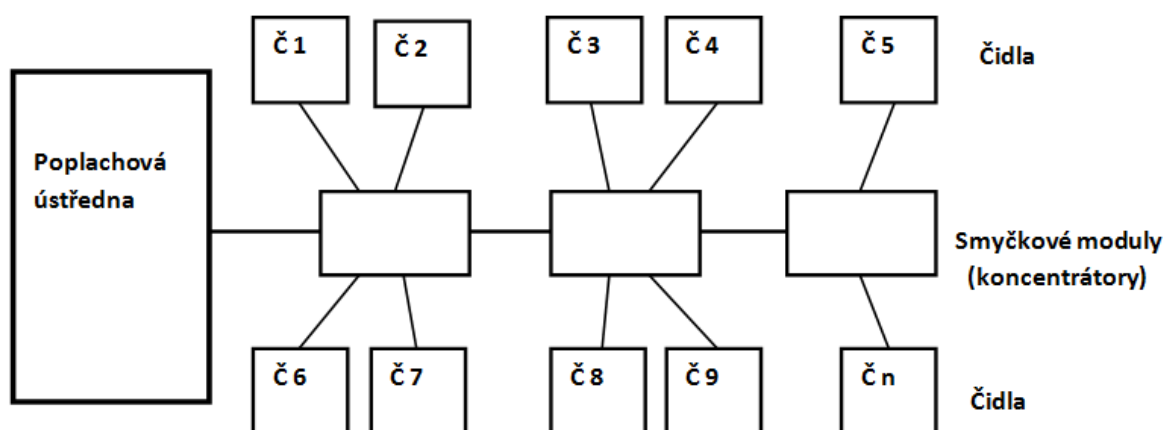


Obr.9 Příklad propojení zabezpečovacího systému se sběrnicovou ústřednou

### 2.5.3 Ústředny smíšeného typu (koncentrátorová)

Ústředna pracuje na principu datové komunikace ústředna – koncentrátor (sběrníkový modul smyček). Pomocí datové nebo analogové sběrnice probíhá komunikace mezi ústřednou a koncentrátory. Pomocí smyček jsou čidla připojena na koncentrátory jako u smyčkových ústředn. Vlastní vyhodnocování probíhá podle typu ústředny různě. Jednou z variant je analogový multiplex, kdy se připojují na sběrnici jednotlivé smyčky a vyhodnocení impedance smyčky s příslušnou odezvou provádí ústředna. Jinou možností je integrace vyhodnocovací logiky s vyrovnávací pamětí přímo do koncentrátoru. Komunikace pak probíhá čistě v datové podobě.

Pokud je kapacita ústředny dostatečná, lze na jednotlivé vstupy koncentrátoru připojit přímo jednotlivá čidla. Tento typ ústředny takto přechází na ústřednu s přímou adresací čidel se všemi jejími výhodami. Důležitým aspektem návrhu systému zůstává stejně jako u předešlé skupiny ústředn, dostatečná dimenze napájecích i datových vodičů, zvláště u rozsáhlých systémů. [1]



Obr.10 Příklad propojení zabezpečovacího systému s koncentrátorovou ústřednou

### 2.5.4 Ústředny s bezdrátovým přenosem od čidel

Využívají se především při zajišťování historických objektů se vzácnými malbami na omítce nebo kamennými zdmi, které nedovolují vedení kabelů pod nebo na omítce. Ústředny bezdrátové sítě EZS se proto uplatňují při dodatečné instalaci v objektu s minimalizací kabeláže a hrubých montážních prací.



Jako základní prvky těchto systémů existují bezdrátová: [2]

- akustická čidla rozbití skla
- čidla pohybu (PIR - pro svůj nízký odběr)
- univerzální moduly pro připojení libovolných čidel
- stabilní a mobilní ovládací díly
- tísňová tlačítka
- magnetické kontakty
- sirény, majáky, atd [2]

V rámci chráněného objektu se mezi ústřednou a jednotlivými základními prvky přenáší bezpečnostní informace obdobně jako u bezdrátového radiového přenosu: [2]

- jednosměrným přenosem
- obousměrným přenosem

### **Ústředny s jednosměrným rádiovým přenosem**

Problémy těchto systémů jsou v jejich jednosměrné komunikaci kontrolovat nelze spolehlivost bezdrátového přenosu signálu na zvláštních nebo vymezených frekvencích (např. v občanském nebo modelářském pásmu, v pásmu 430 MHz atd.).[2]

Ústředny s jednosměrným přenosem proto nejsou vhodné pro objekty s vysokými riziky.

Ve výjimečných případech lze připustit systém jednosměrného bezdrátového systému u důležitých objektů jako podpůrný ke klasickému vodičovému. Toto lze provést jen v místech, kde není instalace vedení možná, nebo v případech krátkodobé instalace. [2]

### **Ústředny s obousměrným rádiovým přenosem**

Tento systém pracuje v pásmu 430 MHz a je trvale monitorován. Tímto způsobem odstraníme nedostatky jednosměrného radiového přenosu a dosáhneme spolehlivosti spojení, srovnatelného se spojením po metalickém vedení. Systém je adresovatelný (cca 100 adres) a je dělitelný na zcela nezávislé subsystémy. Ovládání je zajištěno pomocí blokovacích zámků nebo přenosového ovládače. Volitelně lze ovládání zajistit ještě číselným kódem. [2]

Přenosový ovládač je vybaven obousměrnou komunikací a je schopen indikovat stav zařízení. Využívá se i při pohybu majitele mimo střežený prostor (např. v zahradě), kdy slouží indikací příchodu osob do střeženého prostoru. Dále můžeme přenosový ovládač využít jako tísňový hlásič pro případ přepadení nebo pro tísňové volání tělesně postižených. Verzi vybavenou náklonovým čidlem (tzv. „mrtvý muž“) lze použít mimo jiné též pro obchůzkovou službu. Přenosný ovládač můžeme vybavit infračerveným vysílačem, který slouží ke znemožnění uvedení zařízení do stavu externího střežení, dokud obsluha není uvnitř střeženého objektu. K tomu je použito zvláštní pasivní infračidlo, které se montuje uvnitř střeženého objektu. [2]

Při obousměrném přenosu pracuje systém souběžně na dvou kmitočtech. Pokud dojde k záměrnému narušení nebo atmosferickému rušení jednoho z kmitočtu je schopen si sám vyhledat z dostupného kmitočtového plánu jiné dva pracovní kmitočty. Je vybaven indikací intenzity pole. Takto zjistíme, zda pracuje s dostatečnou rezervou nebo na hranici citlivosti. Přenos mezi jednotlivými prvky je digitální. Je kódován a zabezpečen plovoucím kódem proti odposlechu. [2]

### **Zhodnocení bezdrátové sítě EZS**

Mezi výhody bezdrátové sítě EZS patří zkrácení doby montáže a velká flexibilita. Systém je vhodný i pro dočasné použití. Z tohoto důvodu není problém jej znovu instalovat na nové místo. Flexibilita je dána také konstrukcí. Ústřednu můžeme umístit např. poblíž vchodu a propojit ji s blokovacím zámkem nebo jiným spínacím zařízením. Ústřednu můžeme umístit i na půdu tím způsobem, že se na ni přímo napojí siréna a maják. V neposlední řadě lze maják i sirénu připojit pomocí bezdrátové jednotky a blokovací zámek pomocí bezdrátového ovládacího panelu. [2]

Mezi nevýhody řadíme skutečnost, že čidla a další prvky EZS, které jsou vybaveny bezdrátovým rádiovým vysílačem nebo přijímačem jsou doplněny vlastním napájením (vnitřní baterie). Napětí baterie je kontrolováno. Při poklesu napětí dojde k místní akustické signalizaci nebo tato informace je přenášena do poplachové ústředny. Tím upozorní obsluhu na nutnost její výměny. Zařízení stupně zabezpečení 3 a 4 není možné po signalizaci vyčerpání napájecích baterií zapnout do střežení aniž by byly baterie vyměněny. [2]

Doporučujeme tzv. dvoustupňovou signalizaci:

- a) upozornění
- b) signalizace vybití. [2]

Ze strany výrobců je dána několikaměsíční záruka na provoz baterie. U systémů bez pravidelného testování je záruka několikaletá. Tyto bateriové zdroje je však nutno udržovat pravidelným servisem v provozním stavu. Celkově lze konstatovat, že bezdrátová přenosová zařízení ušetří čas i prostředky, zvýší se však provozní náklady o cenu baterií a pravidelný servis. [2]

V současné době se při zavádění bezdrátových systémů používá přenosů v tzv. rozprostřeném spektru. Tyto systémy se vyznačují vysokými výhodami radiového přenosu informací. Vynikají extrémně nízkými energetickými nároky a zvýšeným dosahem. K jejím výhodám rovněž patří prakticky nemožná rádiová paralyzace spojení a velmi obtížná identifikace činnosti bezdrátového čidla v rádiovém spektru. Jsou velmi perspektivním a mnohdy prioritně nasazovaným prvkem, zejména u objektů zvláštní důležitosti a to i přes vyšší pořizovací náklady. [2]

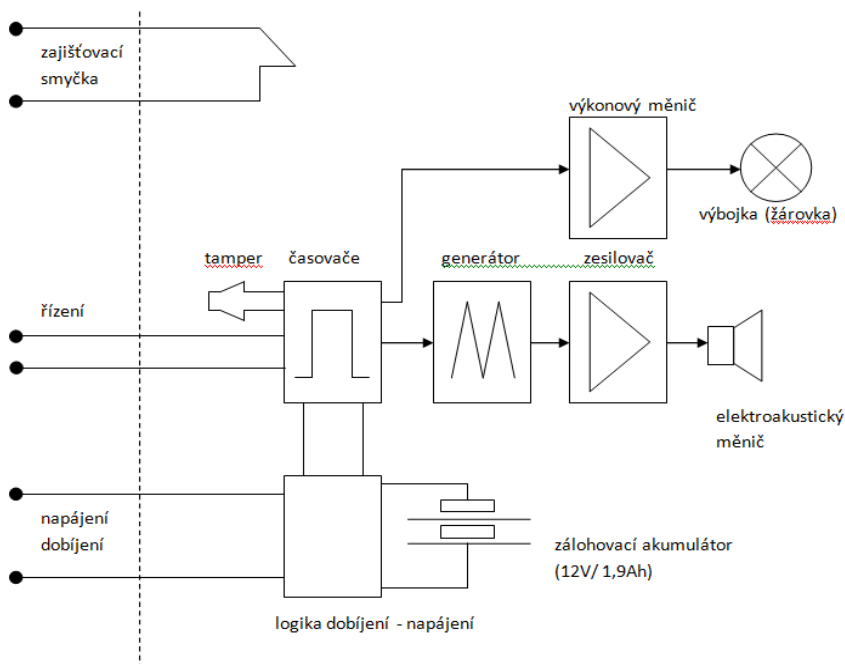
### 2.5.5 Ústředny hybridní

Tato skupina hybridních ústředen se začíná rozvíjet teprve v současné době. Hybridní ústředny umožňují kombinované připojení pomocí klasických drátových vstupů, ale i bezdrátových adresovatelných prvků a lze je ovládat systémovou nebo bezdrátovou klávesnicí. [2]

Nevýhody hybridních ústředn jsou v rozsáhlé kabeláži, neadresovatelnosti jednotlivých prvků apod. K výhodám patří rychlá a snadná montáž, adresovatelnost prvků atd. Tyto ústředny mají vestavěný kombinovaný komunikátor, který přenáší hlasové zprávy, komunikují s PCO a umožňují dálkový přístup do zabezpečovacího systému. Pro svou flexibilitu se zejména používají v objektech, kde v některých prostorách lze použít kabelový rozvod, ale v ostatních vzhledem k jejich charakteru ne. [2]

### 2.5.6 Akustická signalizace

Akustická signalizace je nejčastěji instalovaným doplňkovým zařízením. Provádí se ve dvou variantách, pro interní nebo externí použití. Akustický měnič (dynamický nebo piezoelektrický) doplněný generátorem kolísavého tónu a výkonovým zesilovačem je základem těchto provedení. V malé míře jsou využívány sirény s motorovým pohonem. Akustický výkon je stanoven v technických požadavcích na zařízení. Omezena by měla být doba aktivace (norma ČSN EN 50131-1 stanovuje dobu od 90 s do 15 min, s odkazem na národní předpisy). Sirény se nejčastěji umísťují na průčelí střežených objektů ve výškách, které jsou nedostupné bez použití žebříku nebo montážní plošiny. V současné době se preferují tzv. „inteligentní“ sirény s vlastním zálohováním. [1]



Obr.11 Blokové schéma inteligentní sirény [1]

Siréna je s poplachovou ústřednou propojena vícežilovým kabelem, který slouží k ovládání řídicího vstupu sirény rozpínacím kontaktem bez potenciálového relé ústředny, popř. výstupem otevřeného kolektoru spínacího tranzistoru, dále slouží k dobíjení zálohovacího akumulátoru a k přivedení sabotážní smyčky sirény. Inteligentní sirény jsou aktivovány v těchto případech:

- regulérní poplach systému EZS
- přerušení kabelového propojení ústředna – siréna
- pokus o odstranění pláště sirény
- pokus o sejmutí sirény ze zdi [1]

Do některých sirén je nainstalován optoelektronický hlídací modul, který má za úkol aktivovat poplach při pokusu o odstavení sirény zaplněním vnitřku např. montážní polyuretanovou pěnou přes akustickou mřížku. Jiné typy sirén řeší tento problém dvojitém krytem speciální konstrukce. [1]

### **2.5.7 Optická signalizace**

U venkovních sirén je optická signalizace (světelný maják) součástí jejich krytu. Z technického hlediska se jedná o 12V výkonovou žárovku buzenou přes elektronický přerušovač nebo o výbojku buzenou z vlastní elektroniky. Barva optické signalizace je oranžová. Řízení by mělo umožňovat časově neomezenou aktivaci v případě vyhlášení poplachu. Smysl tohoto opatření spočívá v možnosti identifikace narušeného objektu i po doznění sirény v případě umístění více střežených objektů nedaleko od sebe. [1]

## **2.6 Napájecí zdroje ústředn**

Nejdůležitější díly elektrických zabezpečovacích ústředn jsou napájecí zdroje, které slouží k napájení elektronických obvodů vlastní ústředny a k napájení všech návazných prvků EZS.

- Základní síťové napájecí zdroje
- Přídavné síťové napájecí zdroje
- Náhradní (záložní) napájecí zdroje [2]

### **2.6.1 Základní síťový napájecí zdroj**

Zdroj dodává stabilizované napětí 12 – 13,8 V, je integrovaný do vlastní ústředny a musí být schopen dodat potřebný proud, který je součtem proudových odběrů všech prvků systému, včetně ústředny, připojených na daný zdroj. Zdroj je dimenzován tak, aby po skončení nejdelšího výpadku sítě 12 nebo 60 hodin byl schopen dodat potřebný proud pro všechny prvky připojeny na zdroj včetně dobíjení připojeného akumulátoru během předepsané doby.[2]

## 2.6.2 Přídavný síťový napájecí zdroj

Používá se v rozsáhlých instalacích EZS. Dodává se v zatížitelnosti od 1 do 10 A. Na vstupu síťového napájecího zdroje je zapojen odrušovací člen pro omezení pronikání rušivých složek napájecí sítě do EZS. Eliminuje tím možnost výskytu falešných poplachů. Proti přetížení nebo zkratu jsou jednotlivé výstupy zdroje jištěny samostatnými tavnými nebo elektronickými pojistkami. [2]

### Využití a činnost základního a přídavného napájecího zdroje

Výstupní napětí 12 – 13,8 V se využívá:

- K napájení vlastních elektronických obvodů ústředny
- Pro dobíjení náhradního zdroje ústředny pomocí regulačních prvků
- K napájení ovládacích klávesnic, pomocných relé, čidel systémů atd. Slouží i k napájení aktivních nebo pasivních sirén a k dobíjení náhradního napájecího zdroje aktivních sirén, napájení externích automatických telefonních komunikátorů a napájení nízkopříkonových optických výstražných zařízení. [2]

Činnost základního a přídavného síťového napájecího zdroje a automatický přechod na náhradní napájení při jejich výpadku se vyhodnocují elektronickými obvody a jsou indikovány na ovládacím panelu ústředny. U ústředn vyšší kvalitativní třídy jsou tyto informace uchovávány v paměti, pokud je EZS ve stavu střežení. [2]

## 2.6.3 Náhradní (záložní) napájecí zdroj

Při výpadku napájecího napětí sítě slouží k zajištění funkce celého EZS. Jako náhradní zdroje se používají bezúdržbové, plynotěsné olověné akumulátory s kapacitou 1,2 – 100Ah. Při výpadku síťového napájení zajišťují spolehlivý provoz zdroje v časově omezeném provozu z náhradního zdroje. [2]

ČSN EN 50131-1 stanoví tyto požadavky:

- U všech EZS musí být náhradní napájecí zdroj, v případě výpadku základního napájecího zdroje, schopen napájet EZS po doby stanovené v tabulce 1.
- U EZS stupňů 3 a 4, které mají poplachový přenosový systém, přenášející stav napájecího zdroje na PCO, je možno snížit dobu, po kterou náhradní napájecí zdroj má napájet EZS, na polovinu doby uváděné v tabulce 1.
- U EZS stupňů 2, 3 a 4 pokud jsou vybaveny doplňkovým napájecím zdrojem s automatickým přepínáním mezi základním zdrojem a tímto doplňkovým základním napájecím zdrojem, potom doba, po kterou náhradní napájecí zdroj má napájet EZS, může být snížena na 4hod. U všech EZS musí být zajištěna indikace situace, kdy

napětí náhradního napájecího zdroje poklesne pod hodnotu požadovanou pro správný provoz EZS. [2]

Tabulka 1. Požadované doby napájení náhradním zdrojem [2]

Typ napájení	Stupeň 1 [h]	Stupeň 2 [h]	Stupeň 3 [h]	Stupeň 4 [h]
Typ A – základní a náhradní zdroj dobíjený EZS	12	12	60	60
Typ B – základní a náhradní zdroj nedobíjený EZS	24	24	120	120
Typ C – základní napájecí zdroj s omezenou kapacitou (baterie)	720	720	720	720

Pro všechny EZS, které mají napájecí zdroj typu A, musí být náhradní napájecí zdroj dobít na 80% své maximální kapacity:

- Pro stupeň zabezpečení 1 a 2 za 72hod
- Pro stupeň zabezpečení 3 a 4 za 24hod [2]

Přechod z jednoho zdroje na druhý musí být automatický a nesmí způsobit poplachový stav. Musí být bez rušivého vlivu na funkci EZS. Životnost akumulátorů je garantována výrobcem na 10 let. Při ročních revizích je však vhodné provádět 1 hodinu akumulátorového provozu pro kontrolu kapacity náhradního zdroje. Posouzení poklesu kapacity se provádí dle vybíjecích charakteristik příslušných akumulátorů uváděných výrobcem. [2]

Při volbě vhodného zdroje nesmíme zapomínat na zákonné požadavky ochrany zdraví a života osob. [2]

## 2.7 Ovládací zařízení, propouštěcí zámky, indikační díly a systémy vstupu

Ovládací zařízení slouží k tomu, aby zabezpečovací systém byl ve stavu střežení objektu nebo ve stavu klidu a tím tak plnil svoji funkci při ochraně objektu. Cílem ovládacího zařízení je umožnit jednoduchou obsluhu s minimalizací možnosti vyvolání planého poplachu. Podle požadavků zákazníka a stupně rizik volíme vhodný typ ovládacího zařízení:

- Blokovací zámky
- Spínací (propouštěcí) zámky
- Kódové klávesnice
- Kombinované indikační a ovládací díly
- Ovládací prvky na základě vstupních (propouštěcích) systémů [2]

### 2.7.1 Blokovací zámky

Blokovací zámky jsou nejbezpečnějším a nejjednodušším druhem ovládacího zařízení. Montují se jako přídatné zámky vstupních dveří. Bezchybnou funkci zabezpečovacího zařízení do stavu střežení nebo klidu zajišťuje vlastní konstrukce zámku. Blokovací zámek nelze uzamknout, není-li systém v pořádku. [2]

V případě poruchy nebo opomenutí obsluhy, elektromagnetická západka znemožní uzamčení blokovacího zámku a tím uvedení systému do stavu střežení. Pokud jde zámek uzamknout, uživatel má jistotu, že je systém v pořádku. Při vstupu do objektu je zabezpečovací systém odblokován, protože uživatel musí nejdříve odemknout, aby mohl vstoupit. Odemknutím blokovacího zámku přejde systém automaticky do stavu klidu. [2]

Užití blokovacího zámku je nejpřirozenějším a nejsnazším způsobem ovládání systému. Je však nejnákladnější. Blokovací zámek lze osadit cylindrickou vložkou nebo jeho součástí může být motýlkový či křížový zámek, odolný proti vyhatání a rozlomení. Zámek je též chráněn celoplošným vodivým meandrem proti odvrtání. Meandr je zapojený do vlastní zajišťovací smyčky. [2]

Elektronicky střeženo je ovládací vedení, nebo je chráněno sabotážní smyčkou podle typu ústředny. Blokovací zámek je jediným druhem ovládání, které nepotřebuje přídatnou optickou nebo akustickou signalizaci. Nevýhodou může být závislost celého systému na autorizovaném klíči, který může být bez větších problémů zneužit neoprávněnou osobou. [2]

### 2.7.2 Spínací (propouštěcí) zámky

Spínací zámky jsou ovládací zařízení, podobná blokovacímu zámku. Jsou však bez blokovací elektromagnetické západky. Jsou využívány k samostatnému odpojování smyček nebo k odpojení pracovního kontaktu čidel. Tím je umožněn vstup povolané osobě do určité části chráněného objektu, aniž by došlo k odpojení ostatních zabezpečených prostor napojených na zabezpečenou smyčku. V případě zásahu na objektu, není-li tento stav na PCO nebo v místě trvalé obsluhy indikován, však přináší riziko možného ohrožení oprávněné osoby. Doporučujeme, aby ovládání spínacím zámek bylo z hlediska uživatele doplněno zpětnou optickou nebo akustickou signalizací otevřené smyčky, která byla vyjmuta ze střežení. [2]

### 2.7.3 Kódové klávesnice

Podle provedení klávesnice lze použít jako ovládací nebo propouštěcí zámek. Nezbytná je přídatná optická nebo akustická signalizace stavu systému.

Kódová klávesnice přináší uživateli riziko v nutnosti zapamatování si správného kódu. Dalším problémem je nutnost občasné změny kódu. Trvalý provoz se stejným kódem vedle rizika vyzrazení vede i k fyzickému opotřebení užívaných tlačítek, což sníží počet možných variant pro potencionálního pachatele. [2]

Z tohoto důvodu jsou moderní klávesnice osazovány prosvětlenými tlačítky. Čísla kláves se generují pseudonáhodně, až po stisknutí aktivací klávesy. Prosvětlené pseudonáhodně rozložené klávesy (čitelné jen pod určitým úhlem) umožňují obsluze volit stejný kód na různých klávesách. Tím se zajistí jejich rovnoměrné opotřebení, znečištění a ztíží se tak dálkové odpozorování potencionálnímu pachateli. K výhodám kódových klávesnic patří u většiny používaných typů možnost využití tísňového kódu v rizikovém okamžiku vstupu do objektu. [2]

### 2.7.4 Kombinované indikační a ovládací díly

Kombinované indikační a ovládací díly umožňují indikovat informace o systému a jeho přizpůsobení požadavkům uživatele. Podle umístění je lze vybavit bezpečnostní vložkou, odolnou proti vyhatání a rozlomení, ochranou proti odvrtání, integrovaným bzučákem a počítadlem poplachů. Kombinované indikační a ovládací díly lze doporučit i pro nejvyšší úroveň rizik. [2]

Pro umístění uvnitř střežené zóny jsou vhodné i kombinované klávesnice s informačními displeji. [2]



Obr.12 Kombinovaná kódová klávesnice s displejem



### **2.7.5 Ovládací prvky na bázi vstupních (propouštěcích) systémů**

Odstranění nedostatků některých ovládacích prvků se zpravidla používají ovládací prvky na bázi vstupních identifikačních médií, tzv. vstupníky. Tyto prvky plní nejen kontrolní funkci při vstupu osob do objektu, ale jsou využívány k přesné identifikaci a evidenci osob, které provádějí obsluhu EZS (kdo, kdy, jak). [2]

Do kategorie těchto ovládacích prvků – vstupníků řadíme především magnetické, optické, induktivní a čipové karty, ale i další prvky pracující na fyzikálních principech – biometrických (otisk prstu, geometrie ruky, krevního řečiště hřbetu ruky, obraz duhovky, obraz oční sítnice, hlas, podpis apod.). [2]

## **2.8 Prvky tísňového hlášení**

Slouží k ochraně zaměstnanců a veřejnosti v případě přímého ohrožení. Hlášení do místa pomoci, je vyvoláno přímým manuálním aktem nebo zprostředkovaně při definovaném způsobu manipulace, popř. automaticky bez jakéhokoli přispění obsluhy.[1]

### **2.8.1 Veřejné tísňové hlásiče**

Jsou to magnetické kontakty nebo mikrospínače, které jsou zapouzdřené v podobě tlačítka. Slouží veřejností nebo klientele k vyvolání tísňového hlášení. Jsou situovány na viditelných místech objektů (na schodištích, v chodbách nebo halách) tak, aby je mohl použít každý, kdo je v nouzové situaci.

Veřejné tísňové hlásiče jsou opatřeny krycím sklem, které je při vědomé aktivaci nutné rozbít. Sklo slouží jako ochrana před náhodným použitím (znesnadnění zneužití). Falešné poplachy jsou tak eliminovány na minimum. [1]

### **2.8.2 Speciální tísňové hlásiče**

Jsou to magnetické kontakty nebo mikrospínače v podobě vhodně tvarovaného tlačítka nebo nožní spínací lišty. Slouží k obsluze (zaměstnancům) k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení. [1]

### **2.8.3 Automatické tísňové hlásiče**

Jejich provedení umožňuje vyhlášení tísňového poplachu nezávisle na obsluze – respektováním požadavků případného útočníka. Je to speciální druh tísňových hlásičů, který tvoří tzv. čidla poslední bankovky. Tyto hlásiče se vyrábějí v provedení:

- kontaktní (mechanická) čidla
- bezkontaktní (optoelektronická) čidla

Mechanické kontakty jsou přizpůsobené zasunutím bankovky do pouzdra. Optická čidla pracují na principu reflexního optoelektronického vazebního členu bezkontaktně. To je zárukou dlouhodobě spolehlivé funkce.

Tři varianty optických čidel:

- základní
- s optickou identifikací
- s nastavitelným zpožděním poplachu. [1]

#### **2.8.4 Osobní tísňové hlásiče**

Osobní tísňové hlásiče pracují bezdrátově. Jejich výstupní signál je vysílán do prostoru a modulován kódem shodným s přijímací stranou. Pracují v kmitočtových pásmech 27 MHz, 300 MHz nebo 400 MHz. Další varianty pracují na ultrazvukovém principu. Svým provedením se podobají dálkovému ovládání autoalarmu nebo malým pagerům. [1]

### **2.9 Přenos po síti GSM**

V současné době dochází k rozšíření přenosu na PCO (pult centralní ostrahy) prostřednictvím sítě GSM (Global System Mobile Communication). Tento přenos je relativně levný a jeho velkou výhodou je dobré pokrytí území signálem. Toto řešení umožňuje zabezpečit rychlý přenos (do cca 10 s) informaci na požadované místo. Při relativně vysokém stupni bezpečnosti přenosové trasy. Takovýto přenosový řetězec je tvořen objektovým zařízením, které je instalováno ve střeženém objektu a transformuje požadované informace EZS na formát vhodný k přenosu po síti GSM. Z objektového zařízení je signál přenášen po síti GSM do mobilního telefonu uživatele nebo na pult centralizované ochrany, který přijímá a vyhodnocuje signály z GSM sítě. Síť GSM však není budována pro tento účel a nemá proto odpovídající stupeň spolehlivosti. Na rozdíl od speciálních jednoúčelových sítí je velkou nevýhodou, že jde o síť provozovanou jiným subjektem. Provozovatel sítě GSM negarantuje trvalou provozuschopnost ani dokonalou prostupnost. Na základnových stanicích je třeba provádět údržbu a změny softwaru, což způsobuje, že po určitou dobu není síť v určité oblasti v provozu (v nočních hodinách). [2]

Využívání přenosu systémem krátkých zpráv SMS není pro přenos poplachových zpráv vhodné. I když většinou zpráva dojde relativně brzy stává se, že zpráva dojde se značným zpožděním nebo vůbec. Služba SMS není konstruována pro přenos tak významných informací, jako jsou zprávy o poplachu a neumožňuje přidělení priority pro tyto zprávy.

Důležitým bodem je při využívání GSM zvolit vhodný typ přístroje. Aplikace využívající běžné mobilní telefony, je výhodná z cenového hlediska, je vhodná pro objekty s nízkými riziky. Pro dosažení vysoké bezpečnosti střežených objektů jsou proto vyráběna tato objektová zařízení s důrazem na vysoký stupeň provozní spolehlivosti a přenosové bezpečnosti informací. Používají se pro instalace k ochraně objektů se střeními až vysokými riziky (stupeň zabezpečení 3 a 4). [2]

Komunikační modul GSM AM-PCO je určen k monitorování jednotlivých stavů objektu prostřednictvím nezávislých vstupů. Na základě jejich aktivace dojde k přenosu předem zvolených SMS zpráv nebo hlasových zpráv na určená telefonní čísla. [2]

Kromě komunikace ve směru GSM AM-uživatel, umožňuje komunikátor i zpětnou komunikaci od uživatele k objektu. Toto spojení je schopno provádět dotazování na stav komunikátorů a lze na něm dálkově textovými SMS zprávami nebo tónovou volbou z běžného telefonního přístroje ovládat 4 bezpotenciálové výstupy, kterými lze řídit například hlasové sirény, topení, osvětlení, zavlažování nebo jiná zařízení. [2]

Největší výhodou komunikátorů GSM AM je jeho nainstalování uvnitř střeženého prostoru včetně antény a zabezpečení rychlého přenosu informace. Tím je dosaženo přiměřené bezpečnosti chráněného objektu. Komunikátor dále umožňuje provádět pravidelná kontrolní volání nebo odpovídat na dotaz o svém stavu. Provozně zabezpečuje odesílání zprávy o:

- Výpadku a obnovení napájecího napětí
- Poruše záložního akumulátoru komunikátoru
- Stavů vstupu a výstupu
- Hodnotě zbývajících kreditů u GO a TWIST aktivací
- Úrovní sítě signálu GSM na komunikátoru [2]

Informace zasílané komunikátorem GSM AM lze v praxi přenášet přímo na mobilní telefon, např. majiteli objektu, pověřené osobě, apod. a současně na pult centralizované ochrany. Takto řešený přenosový řetězec nabízí možnosti kontrolní činnosti samotným uživatelem a rovněž zlepšení jeho kontroly nad celým chráněným objektem. [2]

Každý komunikátor GSM AM komunikuje s tímto pultem prostřednictvím SMS zpráv, které jsou vždy doplněny nezaměnitelným číslem chráněného objektu, od kterého zpráva přichází. Celý komunikační modul GSM AM-PCO je instalován v krytu, který je zabezpečen proti neoprávněnému otevření nebo demontáži sabotážním kontaktem. Informace o takovémto napadení je automaticky přenesena na PCO. [2]

Napájení celého modulu je zajištěno z hlavního síťového zdroje. Při jeho výpadku dojde k automatickému přepojení na záložní akumulátor. Napájení jsou monitorována a v případě jejich výpadku je odesláno na PCO poruchové hlášení. [2]

## **2.10 Přenos bezdrátový**

Bezdrátové systémy jsou velkým přínosem v aplikacích, které vyžadují přenos širokého spektra informací na mobilní zařízení příjemce. Tento typ přenosu dělíme na:

- Přenos rádiový
- Přenos optický [2]

### 2.10.1 Přenos rádiový

K dalším možnostem přenosu poplachových zpráv na pult centralizované ochrany patří bezdrátový přenos pomocí speciálně vybudovaných jednoúčelových rádiových sítí. Prudký rozvoj těchto sítí začal kolem roku 1992 na povolených kmitočtech pásma 300-345 MHz.

Mezi výhody rádiového přenosu patří jeho nezávislost na velké JTS nebo drahých přímých linkách. Velkou předností je, že celé zařízení je ve vlastnictví provozovatele, který má dokonalý přehled o jeho provozuschopnosti. Jako nevýhodu považujeme poměrně vysokou cenu přenosového zařízení, které musí disponovat dostatečným výkonem. To vede ke skutečnosti, že mnohé takovéto sítě jsou budovány jako jednosměrné.

Vzhledem k tomu, že lidský organismus rádiové vlny přímo neregistruje, vzniká zdání, že takovýto způsob přenosu poplachových zpráv je ideální. Stinnou stránkou je však to, že takovýto přenos lze snadno rušit, aniž by bylo nutné vstoupit do zabezpečeného prostoru. Pokud pachatel umístí do blízkosti přijímací antény širokopásmový rozmítaný vysílač dostatečného výkonu, dojde k výpadku příjmu ze všech napojených objektů. V tomto případě sice obsluha PCO zjistí, že nemá příjem ze žádného chráněného objektu, nemá však možnost zjistit, který objekt je ohrožen. [2]

K rušení přenosů může docházet i neúmyslně, zvláště v průmyslových oblastech, kde zdrojů rušení je velké množství. Z toho důvodu lze přerušení cesty indikovat až po větším počtu nepřijatých kontrolních relací. Zjištění formátu přenášených zpráv a vysílacího kmitočtu je snadné díky tomu, že přenosová cesta je často kontrolována a není tedy problém zprávu odposlechnout a díky výkonnému PC dešifrovat.

Při rádiovém přenosu informace musíme zvážit řadu ovlivňujících faktorů /např. dosah, stupeň zabezpečení, spolehlivost atd./, vyžadujících specifický přístup k jednotlivým hlediskům, jako jsou výkon, druh provozu, anténní systém apod. Ze všech těchto hledisek se jako optimální řešení jeví přenos v rozprostřeném rádiovém spektru. Přenos bezpečnostních informací v rádiovém spektru dělíme na:

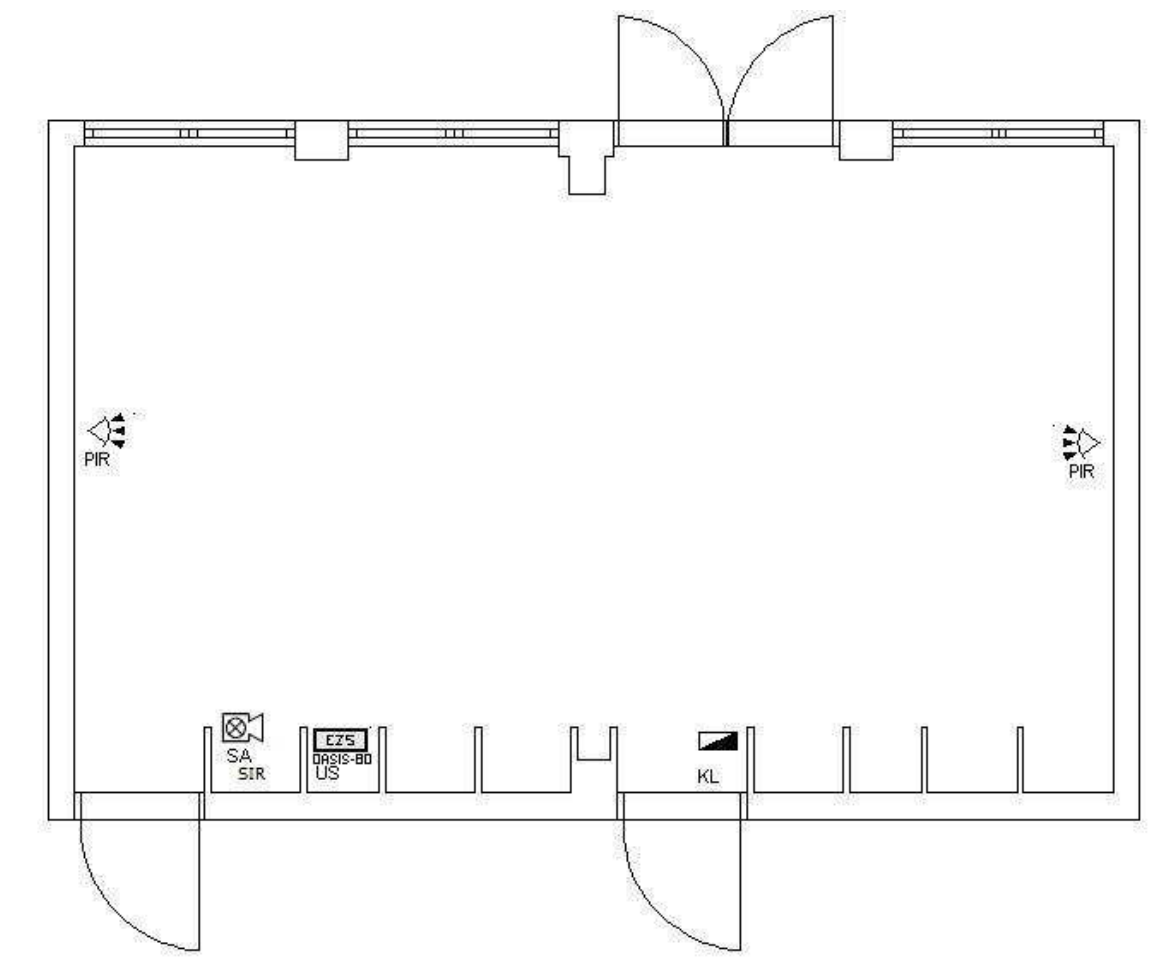
- přenos z objektu na stacionární nebo mobilní stanoviště PCO
- přenos v rámci objektu[2]

### 2.10.2 Přenos optický

Při zabezpečování objektů s velkým výskytem širokopásmových rušivých signálů /např. obráběcí stroje s NC, elektrárenské trafostanice aj./ se v ojedinělých případech užívá infračervené přenosové trasy. To má všechny výhody i nevýhody optického infračerveného přenosu volným prostorem. [2]

### 3. Praktická část





#### 3.1.1 Technická dokumentace EZS



Obr. 13 Technická dokumentace EZS

### 3.1.2 Schématické značky

Tabulka 2. Schématické značky použité v technické dokumentaci EZS

Sch. značka dle ČSN 50131	Popis prvku
	PIR vějíř
	Vnitřní siréna s blikáčem
	Ústředna EZS
	Ovladač, klávesnice

### 3.1.3 Kalkulace nákladů na EZS

#### Kalkulace nákladů

Ústředna drátová OASIS	JA-82K	1290,00 Kč
Akumulátor zálohovací 12V/2,2A	SA-214/2.2	350,00 Kč
Modul rádiové komunikace ústředny	JA-82R	2520,00 Kč
Komunikátor GSM	JA-80Y	5891,00 Kč
Bezdrátová klávesnice	JA-81F	2420,00 Kč
Siréna interní bezdrátová	JA-80L	1114,00 Kč
Modul pro odesílání snímků	JA-80Q	550,00 Kč
Detektor PIR bezdrátový	JA-80P	1318,00 Kč
Detektor PIR bezdrátový s kamerou	JA-84P	2680,00 Kč
Kupón TWIST		336,00 Kč
Karta TWIST		76,00 Kč
Sleva	10%	-1854,50 Kč
Zaokrouhlení		0,33 Kč
Součet položek zdanitelných 20% (základ DPH)		16690,83 Kč
Daň z přidané hodnoty 20%		3338,17 Kč
Celkem		20029,00 Kč

## 4. Závěr

V teoretické části bakalářské práce charakterizují obecné zásady návrhu EZS a specifické požadavky pro střežené objekty. Možnosti integrace EZS se budou dál rozšiřovat mezi movitější vrstvu obyvatel a velkých firem, kde je integrace ochrany osob, majetku a dalších procesů velkou nutností.

Pravděpodobně se bude stále více rozšiřovat efektivní ochrana objektů pomocí EZS. Stupeň účinnosti těchto systémů je úzce spjatý s jejich kvalitou. Efektivnost souvisí s hlediskem společenského a bezpečnostního přínosu.

V praktické části jsem použil pro zabezpečení laboratoře E 118 na VŠB-TU Ostrava elektrický zabezpečovací systém JABLOTRON OASIS 868 MHz, který je koncipován jako bezdrátový systém a díky tomu je jeho instalace snadná. Případné narušení objektu, sabotáž a veškeré dění systému je reportováno pomocí SMS zpráv do mobilního telefonu uživatele popř. na PCO.

Na tento systém lze také připojit kabelem klasické prvky.

Drátové a bezdrátové periferie je možno libovolně kombinovat. Je tedy možná jak zcela bezdrátová, tak drátová nebo kombinovaná sestava. OASIS 868 MHz je stavebnice, ze které lze systém dle požadavků realizovat na míru.

## 5. Literatura

[1] KŘEČEK, Stanislav a kolektiv *Příručka zabezpečovací techniky*. 3. aktualiz. vyd. Blatná : Blatenská tiskárna, 2006. 313 s s. ISBN 80-902938-2-4.

[2] UHLÁŘ, Jan. *Technická ochrana objektů. II. díl : Elektrické zabezpečovací systémy II*. Vyd. 1. Praha : Vydavatelství Policejní akademie ČR, 2005 . 229 s. ISBN 80-7251-189-0.

[3] JABLOTRON ALARMS a.s. *Uživatelský manuál OASiS : MKE22100*. Jablonec n.N. : JABLOTRON ALARMS a.s., 2010. 18 s.

[4] JABLOTRON ALARMS a.s. *Uživatelský manuál OASiS - GSM komunikátor : MFJ 54001*. Jablonec n.N. : JABLOTRON ALARMS a.s., 2010. 16 s.



## 6. Přílohy

### 6.1 Uživatelská příručka

#### **Zajištění systému**

Stiskem klávesy ABC

Zadáním kódu (přiložením karty)

#### **Odjištění systému**

Zadáním přístupového kódu (přiložením karty)

#### **Vypnutí poplachu, zrušení signalizace poplachu**

Zadáním přístupového kódu (přiložením karty)

Signalizace poplachu – blikající ! a údaj o příčině lze zrušit (po vypnutí poplachu) stiskem klávesy #.

Paměť posledního poplachu se zobrazí zadáním \*4, mezi předchozími poplachu můžeme listovat opakovaným stiskem tlačítka 4. [3]

#### **Tísňový poplach**

Na klávesnici zadáním \* 7 kód (karta).

Pokud je systém zajištěn, zároveň se odjistí = ovládání pod nátlakem

#### **Změna a nastavení přístupových kódů**

Master kód (karta)

Je ovládací kód (karta) s vyšší prioritou, pomocí kterého lze ovládat systém a také nastavovat ovládací kódy pro ostatní uživatele. Z výroby je nastaven Master kód: 1234.

Master kód používá majitel nebo správce systému, který si po převzetí systému změní kód z výroby (1234) na svůj osobní master kód nebo kartu . [3]

#### **Změna master kódu (karty):**

Nastavení master kódu (karty) je možné, pokud je systém zcela odjištěn (nesmí být v režimu údržby)

Provede se zadáním:

\* 5 1234 xxxx xxxx

Kde: 1234 je původní master kód

xxxx nový master kód

Kód musí mít 4 cifry, pro kontrolu musí být zadán 2x stejně.

MASTER kód (karty) nelze smazat.

Příklad:

Změna původního master kódu 1234 na nový 7584 zadáním \* 5 1234 7584 7584

Chcete-li místo master kódu používat kartu, zadejte \* 5 původní master kód a přiložte kartu.[3]

### **Nastavování a rušení ovládacích kódů (karet)**

Kódy (karty) lze nastavovat jen pokud je systém zcela odjištěn (nesmí být v režimu údržba)

Ovládací kód (karta) se nastavuje zadáním:

\* 6 xxxx nn yyyy

Kde: xxxx je master kód

nn je pozice kódu 01 až 50

yyyy je nový kód. Zadáním 0000 se kód na pozici nn vymaže.

Příklad:

Při master kódu 1234 nastavíme kód na pozici š. 5 na kombinaci 6793 zadáním:

\* 6 1234 05 6793

Při master kódu 1234 nastavíme kartu na pozici 24:

\* 6 1234 24 přiložení karty. [3]

### **Reportování událostí na telefon**

Telefonní čísla se do paměti M nastavují v režimu Servis zadáním:

81 M xxx...x \*0

Kde: M je číslo paměti 1 až 8

xxx...x je telefonní číslo (max 20 číslic)

Příklad:

zadáním 81 5 777 777 777 \*0 se číslo 7777777777 uloží do paměti 5

Vymazání čísla z paměti M se provede zadáním 81 M \*0

Poznámka: zadáním \*9 před první cifrou čísla se vloží "+" pro uložení čísla v mezinárodním formátu. [3]

### **Přepnutí systému do režimu Údržba**

Do režimu Údržba lze systém přepnout jen, je-li zcela odjištěn – zadáním:

\* 0 master kód (karta). Na displeji se objeví nápis Údržba. [3]

V režimu Údržba lze:

- testovat funkci detektorů a ovládačů
- prohlížet které pozice kódů a karet jsou obsazeny
- vypínat detektory (bypass)
- změnit nastavení vnitřních hodin systému
- nastavit automatické zajišťování a odjišťování
- nastavit telefonní čísla pro reportování událostí ze systému (je-li systém vybaven potřebným komunikátorem) [3]
- Režim Údržba se ukončuje stiskem klávesy #. [3]

### **Prohlížení, které pozice kódů (karet) jsou obsazeny**

V režimu Údržba lze zobrazit, které z pozic 01 až 50 jsou obsazeny kódem a kartou.

Postup prohlížení:

- stisknete klávesu 5
- zobrazí se Správa kódu, 01: Kód (či jméno jeho uživatele),
- klávesami ▲ a ▼ lze listovat jednotlivé pozice
- signálka A indikuje nastavený kód, signálka B kartu
- prohlížení kódů a karet se ukončuje stiskem klávesy #. [3]

### **Seřízení vnitřních hodin systému**

Ústředna obsahuje hodiny a kalendář. Systém zapisuje veškeré události do své paměti včetně údaje o čase. Čas události je také uváděn v SMS reportech hlášených ze systému (pokud obsahuje vhodný komunikátor).

Vnitřní hodiny normálně seřizuje montážní technik při instalaci – včetně možnosti automatické změny zimního a letního času – je-li automatika zapnuta, změní se zimní a letní čas v systému vždy 1. dubna a 1. listopadu.

Pokud potřebujeme hodiny seřídít, můžeme v režimu Údržba zadat:

4 hh mm DD MM RR

Kde:	hh	hodiny
	mm	minuty
	DD	den
	MM	měsíc
	RR	rok (poslední 2 cifry)

Příklad:

Nastavení 21:30 dne 29. dubna 2009 se provede zadáním: 4 21 30 29 04 09. [3]

### **Zajištění systému SMS zprávou**

Tato textová zpráva umožňuje zapnout ústřednu (nebo její část) do hlídacího stavu. Pokud je již systém zajištěn, jeho stav se nezmění.

Odešlete jednoduše SMS s textem: xxxx\_ZAJISTI

Kde: xxxx je platný ovládací kód (uživatelský nebo i Master)  
– oddělující znak mezera

Příklad: Odeslání zprávy 4321 ZAJISTI zajistí systém obdobně jako zadání kódu 4321 na klávesnici EZS.

Poznámky:

- Z výroby je nastaveno, že po zajištění příkazem ZAJISTI potvrdí systém vykonání příkazu zpětnou SMS.
- Nelze-li systém ovládat (např. je v programovacím režimu) komunikátor pouze vrátí zprávu o stavu systému.
- Je-li systém rozdělen, ovládá se ta sekce, do které kód patří. [4]

### **Odjištění systému SMS zprávou**

Tato textová zpráva umožňuje odjistit ústřednu (nebo její část). Pokud je celý systém odjištěn, jeho stav se nezmění.

Odešlete jednoduše SMS s textem: xxxx\_ODJISTI

Kde: xxxx je platný ovládací kód (uživatelský nebo i Master).  
– oddělující znak mezera

Příklad: Odeslání zprávy 4321 ODJISTI odjistí systém obdobně jako zadání kódu 4321 na klávesnici systému.[4]

Poznámky:

- Z výroby je nastaveno, že po odjištění příkazem ODJISTI potvrdí systém vykonání příkazu zpětnou SMS.
- Nelze-li systém ovládat (např. ústředna je v programovacím režimu) komunikátor pouze předá zprávu o stavu systému.
- Pokud je systém rozdělen, ovládá se ta sekce, ke které je kód přiřazen. [4]

### **Zjištění stavu systému pomocí SMS**

Tato textová zpráva umožňuje zjistit aktuální stav zabezpečovacího systému. Komunikátor odpoví zpětnou SMS o aktuálním stavu ústředny, síle signálu GSM, aktuálním připojení na GPRS, úspěšnosti předání na jednotlivá PCO.

Odešlete jednoduše SMS s textem: xxxx\_STAV

Kde:     xxxx           je platný ovládací kód (uživatelský nebo Master).  
          –               oddělovací znak mezera

Příklad: Pokud je systém zajištěn, odpoví po odeslání příkazu 4321 STAV zprávou například: Vas alarm hlasi: Stav systemu: Zajištěno, GSM:3/4, GPRS OK, MS1 OK, MS2 OK. Kde GSM:3/4 znamená sílu signálu GSM 75 a více procent, GPRS OK znamená, že komunikace přes GPRS je navázána a je v pořádku a MS1 OK, MS2 OK znamená, že jsou předány všechny zprávy bezpečnostní agentuře. [4]

### **Zjištění poslední události**

Na tento příkaz komunikátor zareaguje zprávu o poslední události zaznamenané v paměti zabezpečovacího systému.

Odešlete jednoduše SMS s textem: xxxx\_PAMET

Kde:     xxxx           je platný ovládací kód (uživatelský nebo Master).  
          –               oddělovací znak mezera

Příklad: Po poplachu odpoví systém na příkaz 4321 PAMET zprávou: Vas alarm hlasi: Poslední událost: Docasovani poplachu Ustredna Cas: 02.06. 19:48. [4]

### **Zjištění zůstatku na předplacené kartě**

Pokud je v komunikátoru předplacená (dobíjecí) karta, lze se na finanční hodnotu, která je na kartě dotázat.

Odešlete jednoduše SMS s textem: xxxx\_KREDIT

Kde:     xxxx           je platný ovládací kód (uživatelský nebo i Master)  
          –               oddělovací znak mezera

Příklad: Na dotaz xxxx Kredit systém odpoví zprávou: Vas alarm hlasi: Kredit: Vas aktuální zustatek je 476,35Kc.

Poznámka: Tento povel musí být správně nastaven podle operátora. [4]

### Nastavení tel. čísel přenosy

Z výroby je komunikátor přednastaven tak, že pro standardní přenosy SMS a pro akustické zprávy stačí jen nastavit čísla telefonů, na která mají být informace předávány.

Touto sekvencí se nastavují telefonní čísla do sedmi pamětí. Z výroby je pro každé telefonní číslo přednastaveno předání určitých zpráv SMS a předání akustických upozornění. Tím, do které paměti číslo uložíte, volíte, jaké informace bude komunikátor na toto číslo předávat. Uložení tel. čísla do paměti 1 až 7 se provede zadáním:

81 m xxx..x \*0

Kde: M je číslo paměti telefonního čísla 1 až 7  
xxx...x je telefonní číslo (max. 20 číslic), zadáním \*9 lze vložit „+“ pro uložení čísla v mezinárodním formátu, pro použití připojeného SMS telefonu zadejte místo telefonního čísla kód 001

Zrušit vyslání informace na určité číslo lze vymazáním paměti tohoto čísla zadáním:

81 M \*0

Kde: M je číslo paměti telefonního čísla 1 až 7

Příklad: Do paměti 3 uložíte telefonní číslo 603123456 sekvencí stisků: 81 3 603 123 456 \*0.

Sekvencí 813 \*0 číslo z pozice 3 vymažete.

Poznámky:

- Pro přenosy SMS zpráv má smysl zadávat pouze čísla mobilních telefonů nebo čísla call center, na která je možné předávat zprávy SMS.
- Akustické upozornění je možné směřovat jak do mobilní tak do pevné telefonní sítě.
- Komunikátor umožňuje předávat ze zabezpečovacího systému informace o veškerých událostech formou SMS i akustickým upozorněním. Přednastavené přenosy pro jednotlivá telefonní čísla lze změnit nastavením. [4]

### Měření síly signálu GSM

Kvalitní signál GSM sítě je podmínkou správné funkce komunikátoru. Zadáním 922 na klávesnici se zapne měření intenzity signálu. Klávesnice bude zobrazovat úroveň číslem od 0/4 do 4/4. Měření se opakuje každou vteřinu – nový údaj je potvrzen pípnutím. Pro správnou funkci má být úroveň signálu alespoň na stupni 2/4. V místech s problematickým signálem se doporučuje kontaktovat montážní organizaci. Měření se ukončí stiskem klávesy #. [4]

### Zjištění zůstatku pro předplacené karty

Komunikátor umí předat informaci o stavu kreditu předplacené SIM karty. Na zaslání jednoduché SMS s povelom xxxx\_KREDIT komunikátor odpoví textovou zprávou s informací o výši kreditu na předplacené kartě. Před prvním použitím této jednoduché SMS je ale nutno nastavit tvar dotazu na kredit – služby operátora.

Nastavovací SMS zpráva má tvar:

xxxx_KREDIT_*104*#	nastavení pro karty O2 (GO)
xxxx_KREDIT_*101#	nastavení pro karty T-Mobile (Twist)
xxxx_KREDIT_*22#	nastavení pro karty Vodafone (Oskarta)

Kde: xxxx        je platný ovládací kód (uživatelský nebo i Master)  
     \_            oddělovací znak mezera

Pokud chcete hlídat váš zůstatek pomocí SMS zprávy, zadejte povelový řetězec.

xxxx\_KREDIT\_uuu..u\_xx\_yyy\_zz

Kde:   uuu..u        je povel pro zjištění kreditu  
          xx            je perioda zjišťování kreditu ve dnech  
          yyy           je minimální výše zůstatku kreditu  
          zz            je pozice číselné informace o kreditu v SMS od operátora  
          \_            oddělovací znak mezera

Komunikátor se každý xx den sám dotáže operátora na výši kreditu. V odpovědi od operátora prohledává od zz pozice text a jakmile najde číslo (výši kreditu), porovná ji s hodnotou yyy. Pokud je zjištěn kredit nižší nebo roven minimální hodnotě, přenesse se událost „Vybitá baterie GSM komunikátor“ na telefonní čísla s nastavenou událostí „Vybitá baterie“ viz tabulka. Zpráva od operátora se navíc zašle na telefonní číslo 1 a číslo 8, pokud jsou zadána. Pokud je kredit obnoven a je vyšší než minimální, přenesse se událost „Baterie OK GSM komunikátor“. Pravidelné testování se ukončí zadáním povelu bez určení periody.

Příklad: Odesláním 4321 KREDIT 101 # 7 200 1 se bude každý sedmý den od zadání příkazu kontrolovat kredit, na minimální zůstatek 200,-Kč s tím, že číselný údaj o zůstatku kreditu začíná prvním znakem SMS zprávě od operátora.[4]

Poznámky:

- Uživatel je povinen sám se starat o dostatečnou výši kreditu!
- Platnost kreditu na kartě bývá operátorem časově omezena! [4]